EDI

Revista Digital - Distribución gratuita

DICIEMBRE DE 2025 - EDICIÓN N° 42

LA NUEVA ERA DE LOS DINOSAURIOS

ELDERECHOINFORMATICO.COM

SOMOS LA RED

EDI - SONRIE ESTAMOS CREANDO

ELDERECHOINFORMATICO.COM

INDICE

Red Iberoamericana ElDerechoInformatico


SOMOS LA RED
EDI - VEMOS MÁS ALLÁ
ELDERECHOINFORMATICO.COM

EDITORIAL

Este 2025 fue un año complejo, no se que les pareció a Uds, cambios, idas, venidas, tristezas, alegrías, emociones, bah, como casi todos los años, pero este, en particular y desconozco la razón, me ha parecido uno de esos que no pasan en nuestra vida simplemente como un año más, tengo el presentimiento que lo recordaremos por diversas circunstancias por mucho tiempo. EDI ha trabajado sin descanso, su gente ha sido un motor constante de generación de actividades, material académico, propuestas innovadoras

2026 promete, no se sabe que pero promete, esto es algo que también tengo la sensación que por lo charlado, muchos piensan, nos enfrentamos a descubrimientos tecnológicos que nos ponen al límite de nuestras creencias, la IA, la Robótica, los Neuroderechos, entre otras cosas que todavía no conocemos, cosas donde lentamente convergemos. Le pedí a alguien especial que me diga una frase, al azar, sin contexto, algo que le significara algo y me dijo: "Tal vez en otra vida", y creo que en cierta forma definió mucho de lo que pensamos constantemente, tal vez en otra vida vamos a entender que sucede en las redes, tal vez en otra vida, vamos a dejar de buscar lo que no existe y vivir y disfrutar el presente, estamos en la cultura del FOMO, Fear Of Missing Out (miedo a perderse algo), tenemos tanto por delante que no pensamos ni nos damos cuenta lo que dejamos atrás, buscamos siempre el próximo descubrimiento, la próxima IA, los conciertos se viven por celulares, la familia es una videollamada, sin paciencia, sin espera, sin disfrute del hoy, la nueva IA, el nuevo sentimiento, miedo-a-perderse-algo.

GUILLERMO M ZAMORA DIRECTOR-RED ELDERECHOINFORMATICO

Fuimos animales de costumbres y rutinas, esperábamos días por una llamada, cada descubrimiento nos sorprendía, nos interpelaba, nos empujaba a más, ya no, porque todo es ya, es hoy.... Miedo-a-perderse-algo, lo paradójico es que el miedo a perdernos algo que no llego, hace que nos perdamos lo que ya tenemos, el hoy. Felicidades y felices fiestas.

ACOTACIONES BREVES SOBRE EL USO DE LA TECNOLOGÍA Y SU LIMITACIÓN A LOS NIÑOS, NIÑAS Y ADOLESCENTES

Sacha Rohán FERNÁNDEZ CABRERA •

La tecnología es sólo una herramienta. En términos de llevar a los niños a trabajar juntos y motivarlos, el profesor es el más importante.

Bill Gates•

Introducción

Introducción.

Hoy en día es indudable que la tecnología está presente en todos los aspectos de nuestras vidas y a las nuevas generaciones le acompaña desde su nacimiento, siendo que los padres incluso lo usan como instrumento de distracción para sus hijos, a veces de forma educativa, como herramientas para el aspecto académico, entre otros usos.

Este grupo es objeto de protecciones especiales al ser considerados vulnerables, siendo que los países reconocen en sus textos constitucionales y demás normativa interna derechos humanos, fundamentales y constitucionales, para su protección, lo cual, a su vez, se desarrolla en los cuerpos normativos que dictan los cuerpos legislativos de cada Estado. Además, se debe considerar que, esta protección no se limita en el ámbito interno de cada nación, sino que también cuenta con protección internacional como lo son la Convención Internacional sobre los Derechos del Niño,

el cual cuenta además con protocolos facultativos

En el presente trabajo, se hará una reflexión y comentarios puntuales sobre cómo se ha incrementado una tendencia mundial de proteger a los niños, niñas y adolescentes con relación al uso de la tecnología, sin con ello pretender ser exhaustivos en el tema, sino pretendiendo llamar la atención sobre lo que está sucediendo y hacer reflexionar sobre las medidas y corrientes que se están tomando.

1. Protección internacional de los niños, niñas y adolescentes.

Ya mencionamos que cada país dentro de su ordenamiento jurídico establece un sistema de protección para los niños, niñas y adolescentes, siendo que ahora se utiliza este término por recomendación del Fondo de Naciones Unidas para la Infancia (UNICEF) y otros organismos condenan la utilización de la palabra "menor" porque la consideran peyorativa, pero en muchas ocasiones permite reducir la cantidad de caracteres en los títulos.[1] Además, también se recomendó dicha terminología porque dentro de una de las acepciones de la Real Academia Española de la Lengua (RAE) de la palabra menor es "*Que es inferior a otra cosa en cantidad, intensidad o calidad*", no obstante, otro significado de dicha palabra es "*Dicho de una persona: Que tiene menos edad que otra*"[2] y menor de edad lo define como "*Dicho de una persona: Que no ha alcanzado la mayoría de edad*"[3].

Pero en el ámbito internacional, existe también un ordenamiento jurídico que se ha dictado en protección de los menores de edad, como lo son la Convención Internacional sobre los Derechos del Niño y sus Protocolos Adicionales; el Convenio de la Organización Internacional del Trabajo (OIT) N.° 6 Relativo al Trabajo Nocturno de los Menores en la Industria; el Convenio de la OIT N.° 13 sobre la Prohibición de las

[1] Sin embargo, en los "principios éticos" de Unicef para informar acerca de la infancia no se encuentra condena alguna contra la palabra "menor de edad" como se puede apreciar en el apartado II. Estos principios están disponibles en https://centrodocumentacion.psicosocial.net/wp-content/uploads/2004/01/unicef-principios-eticos-informacion-infancia.pdf, consultado el 30/11/2024. En definitiva, lo que parece que se condena es la palabra "menor" a solas y no la compuesta "menor de edad".
El lenguaje se dice que tiene vida y por eso está en transformación constante, las palabras no llegan a nuestro idioma completamente formadas ni en su estado final, sino que el significado de las palabras evoluciona con el paso del tiempo y cambia nuestra percepción del término. Desde un punto de vista sociolingüístico, la aceptación de un cambio lingüístico es socialmente complicado, la lengua refleja la cultura de la sociedad que habla y no al contrario, refleja una sociedad, debiéndose tomar en cuenta que la lengua estándar que es artificial, con ideología y política social, con lo cual se aprecia que la lengua también cambia y manipula a voluntad, buscando reflejar a la sociedad. En definitiva, una palabra con un significado puede cambiar posteriormente, lo que fue una realidad en un momento no significa que lo deba tener ahora, por lo que no escapa del cambio por el tiempo, históricas, sociales (cultismo, semicultismo, elipsis, analogía); por lo que tienen los significados que nosotros le damos, de allí que una palabra será peyorativa según el significado y contexto que le queramos dar.

[2] Tomado de Real Academia Española, https://dle.rae.es/menor, consultado el 30/11/2024.

[3] Tomado de Real Academia Española, https://dle.rae.es/edad#IUJoCCU, consultado el 30/11/2024.

Peores Formas de Trabajo Infantil y la Acción Inmediata para su Eliminación; el Convenio de la OIT N.° 90 sobre el Trabajo Nocturno de los Menores; el Convenio de la OIT N.° 138 Sobre la Edad Mínima de Admisión al Empleo; la Convención Internacional de las Naciones Unidas sobre Represión del Tráfico de Mujeres y Niños; la Convención sobre la Obtención de Alimentos en el Extranjero; el Convenio sobre los Aspectos Civiles de la Sustracción Internacional de Menores; la Convención Interamericana sobre Conflictos de Leyes en Materia de Adopción de Menores; la Convención Interamericana sobre Restitución Internacional de Menores; la Convención Interamericana sobre Obligaciones Alimentarias; el Convenio Relativo a la Protección del Niño y la Cooperación en Materia de Adopción Internacional; la Convención Interamericana sobre Tráfico Internacional de Menores; el Convenio sobre la Ley Aplicable a las Obligaciones Alimenticias Respecto de Menores; el Convenio sobre el Reconocimiento y Ejecución de Decisiones en Materia de Obligaciones Alimentarias; el Convenio sobre Competencia de Autoridades y Ley Aplicable en Materia de Protección de Menores; el Protocolo Facultativo a la Convención sobre los Derechos del Niño sobre un Procedimiento de Comunicaciones; el Acuerdo para la Implementación de Bases de Datos Compartidos de Niños, Niñas y Adolescentes en Situación de Vulnerabilidad del Mercosur y Estados Asociados; entre muchos otros cuerpos normativos sobre la materia.

Así, se puede apreciar que la protección de los derechos humanos (DDHH) de los menores de edad es prolija, con lo cual es evidente que no podía quedar por fuera, que, en algún momento, también se empezara a crear tanto en el ámbito nacional de los países, como en el internacional, normativas en resguardo de los menores de edad. De este modo han aparecido ciertas normas como las Directrices de la UIT sobre la Protección de la Infancia en Línea; la iniciativa Protección Infantil en Línea; la Iniciativa de UNICEF Kindly; la Observación General N.° 25; entre otras que buscan de alguna manera regular estos asuntos y proteger a los niños, niñas y adolescentes.[4]

2. Derecho al uso de las tecnologías.

Vinculado a lo señalado en el punto anterior y vinculado al tema desarrollado, debemos tomar también en consideración lo relativo al derecho de las personas del uso de las tecnologías. De allí, que se hable de un derecho informático o tecnológico que regulan el impacto de las Tecnologías de la Información y Comunicación (TIC) sobre la sociedad, regulando desde los delitos informáticos hasta la protección de la propiedad intelectual o de los datos personales, entre muchos otros aspectos.

En este sentido nos encontramos con la Declaración sobre la utilización del progreso científico y tecnológico en interés

[4] Naciones Unidas, *La seguridad de la infancia y la juventud en la red*, https://www.un.org/es/global-issues/child-and-youth-safety-online, consultado el 13 de mayo de 2025.

de la paz y en beneficio de la humanidad, del 10 de noviembre de 1975, dictada por la Asamblea General de la Organización de Nacionales Unidas (ONU) en su resolución N.° 3384;[5] asimismo está la Resolución sobre la promoción, protección y disfrute de los derechos humanos en internet de la ONU;[6] igualmente existe una Ley Modelo para garantizar el Derecho Humano al acceso a las Tecnologías de la información y la comunicación e Internet y eliminar la Brecha Digital, elaborada por el Parlamento Latinoamericano y Caribeño;[7] por otra parte nos encontramos el Proyecto de Convención Americana sobre Autodeterminación Informativa,[8] entre otros cuerpos normativos existentes, que se vincula también con el Primer Acuerdo Mundial sobre la Ética de la Inteligencia Artificial de la ONU;[9] así como con el Acuerdo sobre Tecnología de la Información (ATI) de la Organización Mundial del Comercio (OMC).[10]

Debemos mencionar también la Asamblea General de la ONU mediante la Resolución 56/183,[11] señaló que "... *el compromiso mundiales necesarios, al más alto nivel político, para promover el inaplazable acceso de todos los países a la información, el conocimiento y la tecnología de las comunicaciones en favor del desarrollo, de manera que se aprovechen todas las ventajas derivadas de la revolución de la tecnología de la información y las comunicaciones, y de abordar todos los temas pertinentes relacionados con la sociedad de la información*..."

Igualmente esta la Declaración de Principios de Ginebra de 2003, también conocida como la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información (CMSI),[12] en la que se

[5] Naciones Unidas, *Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad*, https://www.ohchr.org/es/instruments-mechanisms/instruments/declaration-use-scientific-and-technological-progress-interests, consultado el 13 de mayo de 2025.

[6] CNDH México, *Resolución sobre la promoción, protección y disfrute de los derechos humanos en internet*, https://www.cndh.org.mx/noticia/la-onu-adopta-la-resolucion-sobre-la-promocion-proteccion-y-disfrute-de-los-derechos, consultado el 13 de mayo de 2025.

[7] Parlamento Latinoamericano y Caribeño, *Ley Modelo para garantizar el Derecho Humano al acceso a las Tecnologías de la información y la comunicación e Internet y eliminar la Brecha Digital*, https://parlatino.org/wp-content/uploads/2017/09/plm-garantizar-derecho-acceso-digital.pdf, consultado el 13 de mayo de 2025.

[8] Organización de Estados Americanos, *Departamento de Derecho Internacional (DDI)*, https://www.oas.org/es/sla/ddi/proteccion_datos_personales_Otros_Documentos_CJI.asp, y en Corte Interamericana de Derechos Humanos, *DERECHO DE LA INFORMACIÓN: ACCESO Y PROTECCION DE LA INFORMACION Y DE LOS DATOS PERSONALES (NECESIDAD DE SU REGLAMENTACION INTERNACIONAL)*, https://www.corteidh.or.cr/tablas/14809.pdf, ambos consultados el 14 de mayo de 2025.

[9] Naciones Unidas, *Primer acuerdo mundial sobre la ética de la inteligencia artificial*, https://news.un.org/es/story/2021/11/1500522, consultado el 13 de mayo de 2025.

[10] Organización Mundial del Comercio, *El Acuerdo sobre Tecnología de la Información (ATI)*, https://www.wto.org/spanish/tratop_s/inftec_s/inftec_s.htm, consultado el 13 de mayo de 2025.

[11] Disponible en https://docs.un.org/es/A/RES/56/183, consultado el 15 de mayo de 2025.

[12] Contenida en el Documento WSIS-03/GENEVA/4-S que fuera aprobado el 12 de mayo de 2004, se encuentra disponible en https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html, consultado el 15 de mayo de 2025.

recomienda a las partes el establecimiento de una infraestructura que tenga como elemento esencial la conectividad, teniendo a ésta como un factor indispensable en la construcción de la Sociedad de la Información, siendo que también los Estados deben proveer los siguientes mecanismos a fin de permitir a las personas el acceso y uso de las tecnologías de la información y la comunicación (TIC).

No obstante, se debe aclarar que de la CMSI resultaron dos documentos, la Declaración de principios antes mencionado y un Plan de Acción o WSIS-03/GENEVA/DOC/5-S[13] que complementa al primero, el cual tuvo como finalidad establecer acciones concretas de aplicación de las TIC para que, siendo implementadas por los Estados participantes, contribuyan a superar la brecha digital en que se encuentran.

Existe también una Coalición Mundial para la Seguridad Digital del Foro Económico Mundial[14] que reúne a líderes de varios países con el objetivo de acelerar la cooperación público-privada para hacer frente a los contenidos y conductas nocivos en línea, lo cual obviamente involucra también los niños, niñas y adolescentes, así como su formación. Juntos, los socios en la coalición han desarrollado los Principios Globales sobre Seguridad Digital,[15] cuyo objetivo es ayudar a construir un entorno digital seguro, fiable e inclusivo.

De esta forma se habla del derecho de las nuevas tecnologías, o derecho digital o derecho de la tecnología de la información, referido a un campo legal que se ocupa de las implicaciones legales de la tecnología, especialmente en el ámbito de la información y la comunicación, abarcando una variedad de temas, como la protección de datos personales,[16] la ciberseguridad, la propiedad intelectual en línea y la regulación de Internet,[17] siendo que solamente hemos mencionado unos pocos de los documentos que se han dictado en el ámbito internacional sobre esta materia.

3. Limitación del uso de los celulares, tabletas y otros dispositivos a los menores de edad.

[13] Este fue aprobado también el 12 de mayo de 2004, disponible en https://www.itu.int/net/wsis/docs/geneva/official/poa-es.html, consultado el 15 de mayo de 2025.

[14] Word Economic Forum, *Global Coalition for Digital Safety*, https://initiatives.weforum.org/global-coalition-for-digital-safety/home, consultado el 16 de mayo de 2025.

[15] Word Economic Forum, *Global Principles on Digital Safety: Translating International Human Rights for the Digital Context*, https://www.weforum.org/publications/global-principles-on-digital-safety-translating-international-human-rights-for-the-digital-context/, consultado el 16 de mayo de 2025.

[16] Este es un punto importante dentro de este derecho de las nuevas tecnologías, ya que la recopilación, almacenamiento, transmisión y uso de información personal se han vuelto una constante en la era digital, por lo que la privacidad y la seguridad de los datos es un aspecto primordial, y los gobiernos y organismos reguladores de distintos países han promulgado leyes y regulaciones para abordar estas inquietudes.

[17] Universidad Isabel I, *Qué es el Derecho de las nuevas tecnologías*, https://www.ui1.es/blog-ui1/que-es-el-derecho-de-las-nuevas-tecnologias, consultado el 13 de mayo de 2025.

En relación con el uso de las tecnologías, sus aparatos y su limitación de las instituciones educativas a los menores de edad, debemos mencionar que la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) pidió en el 2023, que se prohibieran los celulares en las escuelas, porque distraen a los alumnos y repercuten negativamente en su aprendizaje, tardando hasta 20 minutos en volver a centrarse en el aprendizaje luego de recibir un mensaje, siendo que la tecnología en la educación solo debe utilizarse cuando haya un beneficio claro para el aprendizaje, porque de lo contrario existe una relación negativa entre el uso excesivo de la tecnología y el rendimiento de los estudiantes.[18]

La UNESCO señaló que, en 14 países, la proximidad del teléfono tuvo un impacto negativo en el aprendizaje, lo que produjo que Bélgica, España y el Reino Unido, optaran por prohibir su uso en las escuelas, obteniendo con ello mejores resultados del aprendizaje. Por ello indicó, que se necesitan directrices claras sobre el uso de la tecnología en las escuelas para evitar daños a la salud de los alumnos y a la sociedad en general. Por eso, es por lo que recomendó que se use la tecnología en las aulas cuando apoye los resultados del aprendizaje, pero sin emplearlo en exceso o de forma inadecuada, sino que la tecnología debe apoyar o complementar, mas no suplantar, la conexión humana en la que se basan la enseñanza y el aprendizaje, sin eliminar el contacto humano y, buscando proteger la privacidad de los datos en la educación y evitar el odio como el acoso escolar o "bullying".[19] Para esto cada país deberá garantizan explícitamente por ley la privacidad.

Este artículo de la UNICEF indica que las investigaciones realizadas, indican que un mayor tiempo frente a la pantalla se ha asociado a un peor bienestar, menos curiosidad, autocontrol y estabilidad

[18] Word Economic Forum, *Por qué la UNESCO pide que se prohíban los celulares en las escuelas*, https://es.weforum.org/stories/2023/08/la-unesco-pide-que-se-prohiban-los-telefonos-en-las-escuelas-por-que/, consultado el 15 de mayo de 2025.
Igualmente, respecto al uso de la tecnología en la educación pidió que se hiciera un uso adecuado ya que se carece de gobernanza y reglamentación adecuadas, por lo que instó a los países a que establecieran sus propias condiciones para el diseño y el uso de la tecnología en la educación, de modo que nunca sustituya a la enseñanza presencial y dirigida por docentes, y apoye el objetivo compartido de una educación de calidad para todos, tomando en consideración si es adecuada, equitativa, ampliable y sostenible. UNESCO, *La UNESCO hace un llamamiento urgente para un uso adecuado de la tecnología en la educación*, https://www.unesco.org/es/articles/la-unesco-hace-un-llamamiento-urgente-para-un-uso-adecuado-de-la-tecnologia-en-la-educacion, consultado el 5 de junio de 2025.

[19] Según la Asociación Española de Pediatría (AEP), haciendo referencia a la UNICEF, el "bullying" se trata de un acoso o agresión para ejercer poder sobre otra persona, compuesto de una serie de amenazas hostiles, físicas o verbales que se repiten, angustiando a la víctima y estableciendo un desequilibrio de poder entre ella y su acosador. Igualmente, destacan que a medida que las dinámicas sociales han ido cambiando a lo largo del tiempo y debido al auge y uso de las tecnologías de la información y de la comunicación como Internet o los teléfonos móviles, los niños están cada vez más expuestos a nuevas formas de acoso. Tomado de AEP, *EL BULLYING O ACOSO*, https://www.aeped.es/sites/default/files/documentos/entrega3_bullying.pdf, consultado el 15 de mayo de 2025.

emocional, mayor ansiedad y diagnósticos de depresión en los niños, niñas y adolescentes. Por ello, la Administración del Ciberespacio de China, ha dicho que los menores de 18 años solo deberían poder utilizar los smartphones un máximo de dos horas al día, además de proponer la implantación de programas para restringir el acceso a Internet de los usuarios menores de 18 años entre las diez de la noche y las seis de la mañana, siendo que los límites de tiempo también los fijarían los proveedores.

Igualmente, se ha de tomar en consideración que la posesión de teléfonos celulares es desigual en todo el mundo, al igual que el acceso a la tecnología en general, con lo cual se produce una desigualdad en el aprendizaje.[20] Casi tres cuartas partes de los mayores de 10 años de todo el mundo poseen uno, pero en los países de renta baja esta cifra se reduce a menos de la mitad.[21] También se calculaba que había un 9% menos de mujeres que de hombres que poseían un teléfono celular para el 2023.[22]

En un informe elaborado recientemente por UNICEF y UNESCO, que fuese entregado el 5 de mayo de 2025, se señala que el 95 por ciento de los niños entre 9 y 17 años tiene acceso diario a un celular con internet, y que el 83 por ciento de los chicos entre 9 y 11 accedió a su primer teléfono antes de los 10 años. Igualmente, el psicólogo Patricio Cabello, académico de la Universidad Andrés Bello y del Centro de Investigación Avanzada en Educación (CIAE) de la Universidad de Chile, indicó que formó parte del equipo que en 2016 presentó el primer informe de Kids Online Chile, que reflejó que la edad media de acceso al primer celular en ese país de Sudamérica era 11 años y que en 2022 repitieron el estudio, y la cifra bajó a los 8, 9 años.[23]

Por su parte, en Francia, luego de que un grupo de especialistas y expertos entregaran al presidente de Francia, Emmanuel Macron, un informe de alerta sobre los peligros que implica el uso temprano de celulares, tabletas y otros dispositivos tecnológicos a temprana edad por parte de los niños, se anunció que ningún infante podrá utilizar teléfonos celulares antes de los 11 años y no tendrán acceso a las redes sociales hasta los 15, esto como una forma de protegerlos ante los riesgos de los cambios de hábitos que

[20] EducaciónDebate, *Crece el debate sobre el uso de los celulares en el ámbito educativo*, publicado el 22/03/2025, https://www.educaciondebate.com.ar/celulares-escuela.html, consultado el 10/06/2025.

[21] Primicia, *ONU: 75% de la población mundial de más de 10 años posee un teléfono*, publicado el 02/12/2022, https://primicia.com.ve/mas/ciencia-y-tecnologia/onu-75-de-la-poblacion-mundial-de-mas-de-10-anos-posee-un-telefono/, consultado el 10/06/2025.

[22] WorldEconomicForum, *Por qué la UNESCO pide que se prohíban los celulares en las escuelas*, publicado el 10/08/2023, https://es.weforum.org/stories/2023/08/la-unesco-pide-que-se-prohiban-los-telefonos-en-las-escuelas-por-que/#:~:text=Tambi%C3%A9n%20se%20calcula%20que%20hay,millones%20de%20d%C3%B3lares%20al%20d%C3%ADa., consultado el 10/06/2025.

[23] Zúñiga, Diego, *Niños con celulares en Latinoamérica: ¿controlar o prohibir?*, publicado en DW el 15/05/2025, https://www.dw.com/es/ni%C3%B1os-con-celulares-en-am%C3%A9rica-latina-controlar-o-prohibir/a-72560243, consultado el 10/06/2025.

puedan padecer, como la falta de lectura, obesidad, entre otros.[24]

De esta manera, ya para el 2019, de manera definitiva los estudiantes menores de 15 años no podían usar sus teléfonos celulares, tableta o relojes inteligentes, en cualquier momento de la jornada escolar, incluyendo el receso, durante el día escolar en las escuelas primarias y secundarias, con algunas excepciones a la prohibición, como la de los estudiantes con discapacidades. Esto para evitar que los estudiantes se vuelvan dependientes y distraídos con sus teléfonos, lo cual está consagrado en la nueva ley nacional que entró en vigencia el 5 de agosto de 2019.[25] Se debe tomar en consideración que la prohibición de teléfonos celulares durante las horas de clase ya estaba vigente desde 2010 con el Código de Educación francés que prohíbe el uso de teléfonos celulares "durante las horas de clase" (esta es la Loi N.° 2010-788 du 12 juillet 2010 portant engagement national pour l'environnement o Ley N.° 2010-788 del 12 de julio de 2010 sobre el Compromiso de la Nación con el Medio Ambiente.[26]

Por otro lado, Reino Unido, realizó una propuesta de ley que pretende endurecer las prohibiciones del uso de smartphones en las escuelas y limitar el modo en que las empresas tecnológicas usan los datos de los niños, la propuesta se presentó en la Cámara de los Comunes el 16 de octubre de 2024 y se debatiría el 7 de marzo de 2025, pero aún no se ha aprobado. El Ministerio de Educación británico ya pide a los colegios que prohíban el acceso a los celulares durante toda la jornada escolar, incluidos el recreo y el almuerzo.[27]

Del mismo modo, en España, en el 2024, se propuso que no se expusiera a la infancia a dispositivos digitales hasta los 6 años, no dar un móvil con conexión a internet hasta los 16 y advertir en el etiquetado de estos aparatos de los riesgos que su uso tiene para la salud. Todas estas son medidas propuestas por el comité creado a petición del Ministerio de Juventud e Infancia, compuesto de 50 personas expertas independientes, para avanzar en la protección de niños y niñas en los entornos digitales y del internet, siendo esto recibido por el Consejo de Ministros.[28]

De allí que, varias comunidades como la de Madrid, Murcia y Cataluña, han

[24] Venezolana de Televisión, *Prohíben el uso de pantallas, celulares y redes sociales a menores en Francia*, publicado el 15/11/2024, https://www.vtv.gob.ve/prohiben-pantallas-celulares-redes-menores-francia/, consultado el 10/06/2025.

[25] Esta prohibición está establecida en la Ley N.° 698 de 2018 o "Loi n° 2018-698 du 3 août 2018 relative à l'encadrement de l'utilisation du téléphone portable dans les établissements scolaires" disponible en Legifrance, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037284333, consultado el 17/06/2025.

[26] Forbes, *Este país es el primero en prohibir el uso de celulares en la escuela*, https://forbes.com.mx/este-pais-es-el-primero-en-prohibir-el-uso-de-celulares-en-la-escuela/, consultado el 10/06/2025.
La ley está disponible en Legifrance, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000022470434, consultado el 17/06/2025.

[27] Wired, *Reino Unido estudia prohibir el uso de smartphones a los niños*, https://es.wired.com/articulos/reino-unido-estudia-prohibir-el-uso-de-smartphones-a-los-ninos, consultado el 09/06/2025.

[28] Corona Gómez, Rosa María, *El comité de expertos aconseja no dar móviles con internet a los menores de 16 años*, publicado en EFE el 03/12/2024, https://efe.com/ciencia-y-tecnologia/2024-12-03/comite-expertos-aconseja-no-dar-moviles-internet-menores-16-anos/, consultado el 10/06/2025.

prohibido el uso individual de ordenadores, tabletas y móviles en las aulas de infantil y primaria.[29]

Dinamarca recomendó prohibir el uso de celulares y tabletas en las escuelas de primaria y secundaria, a estudiantes de entre 7 y 17 años, para mitigar las distracciones en el aula y promover un entorno más propicio para el aprendizaje, implementando esto por una enmienda legislativa, marcando un cambio en su postura previa de no regular el uso de dispositivos móviles en los centros educativos, siendo que el 84% de las escuelas danesas ya cuentan con políticas para regular el uso de móviles.[30]

Tras quince años apostando por las herramientas digitales y haber sido el primero en tomar la iniciativa e introducir estos métodos digitales en sus colegios e institutos en 2009, Suecia decidió volver a los tradicionales libros de texto y retirar los ordenadores de sus aulas. Esto luego de analizar la productividad y resultados de sus alumnos, donde se vio un menor rendimiento escolar debido a una digitalización excesiva, que aunque agiliza los procesos y pone al alcance nuevas herramientas, Internet y las distintas plataformas también genera en los estudiantes numerosas distracciones, además que leer en pantallas retroiluminadas genera más fatiga visual que leer en papel, siendo que estudiar se convierte en un proceso más cansado y pesado, además de provocar problemas de salud, como la miopía o la vista cansada a edades tempranas, junto con que dificulta la concentración en el aprendizaje y genera un deterioro en competencias clave como la comprensión lectora y el análisis crítico de los contenidos. Todo esto tras conocer el Informe Estudio Internacional para el Progreso de la Comprensión Lectora (PIRLS) 2021, desarrollado por la Asociación Internacional para la Evaluación del Logro Educativo (AIE) que evalúa la comprensión lectora y las tendencias de aprendizaje de aproximadamente 400.000 alumnos de 4º grado escolar, o sea, niños de entre nueve y diez años, en centros educativos de 57 países de todo el mundo.[31]

Otros países europeos como Países Bajos, Hungría y Grecia han buscado restringir los teléfonos móviles y otros dispositivos electrónicos en las escuelas durante el año 2023, lo cual refleja la preocupación en toda Europa sobre el impacto de la tecnología en el bienestar de los estudiantes y los resultados educativos.[32]

[29] El País, *Adiós al optimismo tecnológico en el colegio y hola de nuevo al papel y boli*, https://elpais.com/expres/2025-03-21/adios-al-optimismo-tecnologico-en-el-colegio-y-hola-de-nuevo-al-papel-y-boli.html, consultado el 10/06/2025.

consiste la norma y cómo será aplicada, publicado en Infobae el 23/05/2025, https://www.infobae.com/peru/2025/05/23/congreso-aprueba-ley-que-regula-el-uso-de-celular-en-el-colegio-en-que-consiste-la-norma-y-como-sera-aplicada/, consultado el 10/06/2025.

[31] Soto, Rosa, *Suecia revisa la digitalización escolar, pero los expertos avisan de que "es inevitable" introducir la tecnología en las aulas*, publicado en Newtral el 6 de junio de 2023, https://www.newtral.es/por-que-suecia-digitalizacion-escuelas/20230606/, consultado el 10/06/2025.

[32] Min, Roselyne, *Política de "escuelas sin móviles": ¿Cómo funcionan las aulas sin teléfonos de Dinamarca?*, publicado en Euronews el 07/10/2024, https://es.euronews.com/next/2024/10/07/politica-de-escuelas-sin-moviles-como-funcionan-

En Venezuela, el ejecutivo nacional para noviembre de 2024 comenzó una campaña originada por situaciones peligrosas derivadas de los llamados retos virales, especialmente en detrimento de la salud e integridad de la población menor de edad, lo que llevó a que en regiones como el estado Monagas ya se han tomado ciertas medidas al respecto, como la prohibición a los estudiantes de primaria y bachillerato de portar y utilizar teléfonos celulares dentro de las instituciones educativas de la entidad federal.[33]

Por su parte el Congreso de Perú, en mayo de 2025, aprobó el Proyecto de Ley 5532, que regula el uso de teléfonos celulares y otros dispositivos electrónicos en todas las instituciones y programas educativos de la educación básica, durante los procesos de enseñanza y aprendizaje, salvo que los dispositivos sean empleados con fines pedagógicos expresamente autorizados por la institución educativa o en el caso de las excepciones para estudiantes con condiciones de salud que requieran el uso de dispositivos electrónicos como parte de su atención, ante lo cual los directores de las instituciones deberán implementar protocolos específicos para garantizar el cumplimiento de la norma, además de aplicar medidas correctivas bajo criterios de gradualidad, razonabilidad y proporcionalidad, ya que no es una ley punitiva, sino adaptativa a las realidades de cada escuela.[34]

Por otro lado, en Brasil, para enero de 2025, el presidente de la República firmó un proyecto de ley que restringe el uso de teléfonos inteligentes en las escuelas, que se aplicó en las escuelas primarias y secundarias en toda la nación a partir de febrero, permitiendo sólo utilizar dichos dispositivos en casos de emergencia y peligro, con fines educativos, o si tienen discapacidades y los necesitan.[35]

Aunque ya previamente, en noviembre de 2024, el estado de Sao Paulo tuvo una iniciativa de prohibir los celulares en las escuelas, por medio de su Asamblea Legislativa, que aprobó por unanimidad un proyecto de ley que prohíbe el uso de teléfonos celulares y cualquier dispositivo electrónico con acceso a internet durante el período en que los estudiantes estén en las escuelas, tanto públicas como privadas, lo cual incluye descansos y actividades extracurriculares, con excepciones para las actividades escolares determinadas por los profesores o su uso por parte de estudiantes con alguna discapacidad y que necesitan un celular para seguir las clases, así como que las secretarías de educación municipales y estatales deben definir

---

las-aulas-sin-telefonos-de-dinamarca, consultado el 10/06/2025.

[33] Efecto Cocuyo, *Monagas es la primera entidad que prohíbe uso de celulares en las escuelas*, publicado el 25/11/2024, https://efectococuyo.com/la-humanidad/monagas-es-la-primera-entidad-que-prohibe-uso-de-celulares-en-las-escuelas/, consultado el 10/06/2025.

[34] Solar Silva, David, *Congreso restringe el uso de celulares en los colegios de todo el país: ley aplica para instituciones públicas y privadas*, publicado en Infobae el 22/05/2025, https://www.infobae.com/peru/2025/05/23/congreso-restringe-el-uso-de-celulares-en-los-colegios-de-todo-el-pais-ley-aplica-para-insituticiones-publicas-y-privadas/, consultado el 10/06/2025.

[35] Associated Press, *Brasil restringe el uso de teléfonos inteligentes en escuelas primarias y secundarias*, publicado el 13/01/2025, https://cnnespanol.cnn.com/2025/01/13/latinoamerica/brasil-restringe-telefonos-inteligentes-escuelas-ap, consultado el 10/06/2025.

protocolos para almacenar los celulares durante el horario escolar.[36]

En el caso de México, Querétaro, se convirtió en el primer estado en prohibir el uso de dispositivos móviles y celulares en escuelas de nivel básico y nivel medio superior, por parte de los menores de edad para protegerlos de los riesgos que existen en las redes sociales.[37]

En Colombia, para el 2022, el entonces Ministerio de Educación, señaló que el uso de teléfonos celulares por parte de los estudiantes debía ser reglamentado en los manuales de convivencia de los colegios, pero no prohibirlos, pues ellos podían servir como herramienta en los procesos de desarrollo académico. Igualmente, la Corte Constitucional, en sentencia T-967 del 2001,[38] señaló que, aunque las instituciones educativas tienen la autonomía para establecer las reglas que consideren apropiadas para regir las relaciones dentro de la comunidad educativa, del mismo modo deben regular dichas relaciones mediante reglas claras sobre el comportamiento que se espera de sus miembros, así como otorgar las garantías del debido proceso en el ámbito disciplinario. La prohibición de uso de estos equipos tecnológicos se debe realizar de acuerdo con la Ley 2170 del 2021,[39] que autoriza el uso de dispositivos móviles en entornos escolares, indicando que corresponde a la cartera de educación formular, implementar, seguir y evaluar las orientaciones técnicas para el uso de las herramientas de tecnologías de información y comunicaciones (TIC) por parte de los menores de edad en entornos escolares, para los niveles de preescolar, básica y media.[40]

4. Limitación del uso de las redes sociales a los menores de edad.

Observamos que Australia para noviembre de 2024, prohibió el uso de las redes sociales a menores de 16 años, siendo pionera en este tema en el mundo, aunado a que es la legislación de internet más estricta que entrará en vigor este noviembre de 2025, con el objetivo de proteger a las personas jóvenes de los daños de las redes sociales y pide a las empresas tecnológicas que fortalezcan la seguridad antes de una fecha límite.[41]

---

[36] El Venezolano News, *Este país aprueba el primer proyecto que prohíbe el uso de celulares en las escuelas*, https://elvenezolanonews.com/este-pais-aprueba-el-primer-proyecto-que-prohibe-el-uso-de-celulares-en-las-escuelas/, consultado el 10/06/2025.

[37] El mundo del Derecho, *¿Cuál es el primer estado en aplicar ley que prohíbe el uso de celulares en escuelas?*, https://elmundodelderecho.com/cual-es-el-primer-estado-en-aplicar-ley-que-prohibe-el-uso-de-celulares-en-escuelas/, consultado el 10/06/2025.

[38] Sentencia disponible en Corte Constitucional de la República de Colombia, https://www.corteconstitucional.gov.co/relatoria/2001/t-967-01.htm, consultado el 17/06/2025.

[39] Disponible en Sistema Único de Información Normativa, https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043744, consultado el 17/06/2025.

[40] Ámbito Jurídico, *Colegios pueden regular el uso de teléfonos celulares, pero no prohibirlos*, https://www.ambitojuridico.com/noticias/general/constitucional-y-derechos-humanos/colegios-pueden-regular-el-uso-de-telefonos, consultado el 10/06/2025.

[41] Ritchie, Hannah, *Australia prohíbe el uso de las redes sociales a menores de 16 años con la legislación de internet más estricta del mundo*, publicado en la BBC el 29/11/2024, https://www.bbc.com/mundo/articles/cq52v666vl3o, consultado el 09/06/2025.

En Estados Unidos, lo referente a la Normativa de Protección de la Privacidad Infantil en Línea (COPPA, por sus siglas en inglés)[42] tiene como objetivo proteger la privacidad de los menores de 13 años en internet y establece que los padres deben prestar su autorización para el registro de los niños de estas edades en redes sociales, en el parágrafo 312.2. Del mismo modo, paralelamente, cada Estado puede desarrollar sus propias restricciones.

Así es como vemos que, en el 2024, también la Cámara de Representantes de Texas aprobó la HB-186,[43] una norma que prohíbe a cualquier menor de dieciocho años abrir o mantener cuentas en redes sociales y obliga a las plataformas a verificar la edad de todos sus usuarios y a borrar los perfiles infantiles a petición de los padres.[44]

Para el 25 de marzo de 2024, el gobernador de Florida, Ron DeSantis, firmó un proyecto de ley que prohíbe a los menores de 14 años el acceso a las redes sociales.[45]

Ya para abril de 2025, en Carolina del Norte, un grupo de legisladores trabajo en una propuesta de ley para prohibir el uso de redes sociales a menores de edad, ya que, según el representante republicano, Jeff Zenger, el 33% de las niñas de entre 11 y 15 años se han vuelto adictas a las redes sociales, lo que representa un mayor riesgo para desarrollar depresión y ansiedad; además de que la mayoría de los menores están expuestos "al acoso cibernético y la sextorsión".[46]

En lo que respecta a la Unión Europea, el Reglamento General de Protección de Datos (RGPD o GDPR, por sus siglas en inglés)[47] europeo requiere el consentimiento de los padres para el procesamiento de datos personales de niños menores de 16 años. Sin embargo, permite a los Estados miembros reducir por ley este límite hasta los 13 años, todo de conformidad con su artículo 8.

Aunque los reglamentos son vinculantes para los 27 países miembros de la Unión Europea, las disposiciones de este cuerpo normativo sobre el consentimiento de los menores para el uso de servicios digitales no interfieren con las leyes desarrolladas individualmente por los Estados al respecto.

Francia en el 2023, dictó una legislación para bloquear el acceso a las

---

[42] Code of Federal Regulation, *Children´s online privacy protaction rule*, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312, consultado el 10/06/2025.

[43] Disponible en Texas Policy Research, *HB 186*, https://www.texaspolicyresearch.com/bills/89th-legislature-hb-186/, consultado el 10/06/2025.

[44] Dans, Enrique, *Prohibir las redes sociales a los menores: un despropósito que multiplica los riesgos*, https://www.enriquedans.com/2025/05/prohibir-las-redes-sociales-a-los-menores-un-desproposito-que-multiplica-los-riesgos.html, consultado el 09/06/2025.

[45] Wired, *Seguimos sin estar de acuerdo sobre el efecto del uso de pantallas en los niños*, https://es.wired.com/articulos/seguimos-sin-acuerdo-sobre-efecto-uso-de-pantallas-en-ninos, consultado el 10/06/2025.

[46] Barrera, Daniela, *Adiós a las redes sociales para menores: En este estado están aprobando una ley para prohibirlas*, publicado en el New York Times el 16/04/2025, https://www.nytimes.com/es/2024/11/29/espanol/mundo/australia-prohibicion-redes-sociales-menores-16.html, consultado el 09/06/2025.

[47] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679, consultado el 10/06/2025.

redes sociales de niños menores de 15 años que no tuvieran el permiso de sus padres, igualmente se obliga a las compañías digitales a verificar la edad de sus usuarios y a activar un sistema para controlar el tiempo de permanencia online de los niños y adolescentes, entre otras medidas.[48]

En España se considera que un adolescente a partir de los 14 años tiene la capacidad de consentir por sí mismo el tratamiento de sus datos, según el artículo 7 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.[49] Igualmente, el Consejo de Ministros español aprobó en junio de 2024, un anteproyecto de ley para la protección de los menores en los entornos digitales, que propone elevar de los 14 a los 16 años la edad mínima para abrirse una cuenta en redes sociales sin el permiso parental, la publicidad dirigida a menores y el uso de dispositivos en los centros educativos, entre otros aspectos.[50]

Italia, también exige a los menores de 14 años el consentimiento expreso de sus padres o tutores legales para registrarse en redes sociales, mientras que a partir de esa edad no es necesaria esta autorización.[51]

En Chile existe un proyecto de Ley que Prohíbe el Acceso y Utilización de Cuentas de Redes Sociales a Menores de Catorce Años, presentado en la sesión N.° 126 el 13 de enero de 2025 para el período legislativo 2022-2026.[52]

Igualmente, según Adrián Moreno, señaló que "las redes sociales han desarrollado diversas restricciones para proteger a los menores, en cumplimiento de regulaciones internacionales", aunque no son suficientemente efectivas.[53]

5. Reflexiones finales.

[48] Vie publique, *Loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, publicado el 10/07/2023, https://www.vie-publique.fr/loi/288274-majorite-numerique-15-ans-reseaux-sociaux-loi-7-juillet-2023#:~:text=Panorama%20des%20lois-,Loi%20du%207%20juillet%202023%20visant%20%C3%A0%20instaurer%20une%20majorit%C3%A9,contre%20la%20haine%20en%20ligne&text=Pour%20prot%C3%A9ger%20les%20enfants%20des,en%20place%20une%20solution%20technique)., consultado el 10/06/2025.

[49] Disponible en el Boletín Oficial del Estado, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673, consultado el 10/06/2025.

[50] La Moncloa, *PROTECCIÓN DE MENORES EN ENTORNOS DIGITALES*, https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2024/20240604-referencia-rueda-de-prensa-ministros.aspx#menores, y en Cánovas Morillo, Carlos, *La futura ley de protección a menores eleva de 14 a 16 años la edad mínima para abrirse una cuenta en redes*, publicado en Newtral del 05/06/2024, https://www.newtral.es/anteproyecto-ley-proteccion-menores-entorno-digital/20240605/, consultados el 10/06/2025.

[51] Corriere della Sera, *La tutela dei minori online: sfide e soluzioni nella giungla normativa*, https://www.corriere.it/tecnologia/24_ottobre_12/la-tutela-dei-minori-online-sfide-e-soluzioni-nella-giungla-normativa-f67e8329-a579-46a3-a014-fcf047fb3xlk.shtml, consultado el 10/06/2025.

[52] Disponible en Cámara de Diputadas y Diputados, https://www.camara.cl/verDOC.aspx?prmID=81923&prmTipo=FICHAPARLAMENTARIA&prmFICHATIPO=DIP&prmLOCAL=0, consultado el 17/06/2025.

[53] Soto, Rosa, *De los 13 a los 16 años, así regulan los países la edad de acceso a las redes sociales*, publicado el 29/11/2024,

Sin duda alguna, la tecnología está presente en muchas de las actividades cotidianas de los seres humanos, si no, en casi todas, ya sea de manera directa o indirecta. Por lo tanto, en el proceso formativo y educativo de los seres humanos, sin duda alguna también se utilizan las TIC y en algunos casos las IoT.

En tal sentido, se deben tomar en cuenta como herramientas que pueden facilitar el acceso al aprendizaje y una manera más rápida y efectiva para aprender, pero sin que, con ello, se dejen de utilizar otros métodos que coadyuvan al crecimiento intelectual y motor de los niños, niñas y adolescentes y que no pueden ser sustituidos por la tecnología.

Lo anterior cobra aún más sentido cuando observamos noticias como que varios estudios han demostrado que cuando aumenta el uso de la televisión, los videojuegos o los dispositivos digitales en general, el coeficiente intelectual disminuye, según el neurocientífico Michel Desmurget, en su libro "La fábrica de cretinos digitales", mientras que en otros momentos anteriores los investigadores habían observado en muchas partes del mundo que el coeficiente intelectual aumentaba de generación en generación, lo cual ahora ha cambiado.[54]

Dentro de los motivos de tal disminución del coeficiente intelectual se indican la:

> "disminución en la calidad y cantidad de interacciones intrafamiliares, que son fundamentales para el desarrollo del lenguaje y el desarrollo emocional; disminución del tiempo dedicado a otras actividades más enriquecedoras (tareas, música, arte, lectura, etc.); interrupción del sueño, que se acorta cuantitativamente y se degrada cualitativamente; sobreestimulación de la atención, lo que provoca trastornos de concentración, aprendizaje e impulsividad; subestimulación intelectual, que impide que el cerebro despliegue todo su potencial; y un estilo de vida sedentario excesivo que, además del desarrollo corporal, influye en la maduración cerebral."[55]

Igualmente, se debe tomar en consideración que según Manuel Martín-Loeches Garrido, catedrático de Psicobiología en la Universidad Complutense de Madrid, una persona es más o menos inteligente por múltiples factores como el factor biológico o el factor social como un beneficio adquirido de la educación y de la cultura a la que ha sido sujeto, y sobre todo de la acumulación de conocimientos, siendo esto último un factor clave en el desarrollo del ser humano en el empleo o capacidad de solucionar problemas nuevos, lo cual se vincula al efecto Flynn.[56]

---

[54] Hernández Velasco, Irene. *Los 'nativos digitales' son los primeros niños con un coeficiente intelectual más bajo que sus padres*. Publicado en BBCMundo el 28/10/2020, https://www.bbc.com/mundo/noticias-54554333, consultado el 09/06/2025.

[55] Hernández Velasco, Irene. Op. Cit.

[56] Se llama efecto Flynn en honor al investigador neozelandés James R. Flynn,

También, Jonathan Haidt, psicólogo y autor del libro "La generación ansiosa", indica que las instituciones que limitaron el uso de celulares reportan menos problemas de disciplina, menos conflictos entre estudiantes y mayor interacción social entre alumnos, reflejando un ambiente más saludable para el desarrollo de los menores. Del mismo modo indicó que, los jóvenes de la generación Z son conscientes de los efectos negativos de los teléfonos móviles, pero se sienten atrapados en un sistema que fomenta su uso constante.[57]

Conclusiones.

Sin duda la tecnología se usa en casi todos los aspectos de nuestras vidas incluyendo la de los niños, niñas y adolescentes, abarcando también el aspecto escolar y educativo. Por ello, es que varios organismos internacionales y países, han propuesto principios y regulaciones en cuanto al uso de las TICs, he incluso se han dictado normativas de uso, limitación o prohibición del empleo de los dispositivos electrónicos y las redes sociales durante los horarios de clases.

Lo anterior, no ha sido tarea fácil, sobre todo al tomar en consideración que existen actualmente el derecho de las personas al uso de las tecnologías, por lo que se ha de buscar un equilibrio entre el ejercicio de estos derechos, la formación y desarrollo humano, así como la limitación en su justa medida en el caso de los menores de edad, para que no les afecte su desarrollo y su intelecto, pero que además puedan tener los conocimientos necesarios en el uso de estas herramientas, sobre todo al tomar en consideración que su uso irrestricto e ilimitado les afecta tanto en lo físico como en lo psicológico e intelectual.

En definitiva, el debate sobre la presencia y uso de teléfonos móviles y otras tecnologías en los centros educativos es complejo y multifacético, sin respuestas sencillas ni soluciones universales, por lo que prohibir o restringir estos dispositivos debe tomar en consideración los potenciales beneficios en términos de reducción de distracciones y riesgos, frente a las posibles pérdidas de oportunidades educativas y el imperativo de preparar a los jóvenes para un mundo digitalizado.

En este sentido, se deberán tomar en cuenta varios aspectos que se pueden considerar cruciales como: 1) el impacto neurocognitivo, 2) el impacto psicosocial, 3) la eficacia de las prohibiciones, 4) las

quien descubrió y documentó la existencia de un crecimiento constante en el cociente intelectual (CI) de las personas, el cual oscilaba entre dos a tres puntos por década- explica el concepto sobre el que se construye la idea de que los hijos son más inteligentes que sus padres. Toda este párrafo es tomado de BBVA. *¿Las nuevas generaciones son más inteligentes que sus padres? ¿El uso del celular genera adicción?*. publicado el 22/05/2024, https://www.bbva.com/es/sostenibilidad/las-nuevas-generaciones-son-mas-inteligentes-que-sus-padres-el-uso-del-celular-genera-adiccion/, consultado el 09/06/2025.

[57] Rosen, Nazareno, *"En las escuelas que prohibieron los celulares se vuelven a oír risas en los pasillos": consejos de un psicólogo para que los niños dejen las pantallas*, publicado en Infobae el 23/04/2025, https://www.infobae.com/tendencias/2025/04/23/en-las-escuelas-que-prohibieron-los-celulares-se-vuelven-a-oir-risas-en-los-pasillos-consejos-de-un-psicologo-para-que-los-ninos-dejen-las-pantallas/, consultado el 10/06/2025.

tendencias y enfoques globales; y 5) la necesidad de un paradigma integrador.

De allí que se debe determinar si la prohibición de la tecnología en las escuelas es un avance o un retroceso, lo cual dependerá de las medidas que se adopten. Así, la clave, no reside en la prohibición *per se*, sino en el por qué y el cómo se implementa, junto con otras estrategias educativas y de apoyo que le acompañen. Lo ideal sería ir hacia un modelo donde la tecnología se utilice de manera intencional, regulada y pedagógicamente justificada, en paralelo con una sólida y continua educación para la ciudadanía digital, la autorregulación y el bienestar en el entorno *online* y *offline*.

Por eso, los responsables políticos y las autoridades educativas ha de desarrollar directrices flexibles y basadas en evidencias que permitan promover marcos regulatorios que ofrezcan orientación, pero que permitan a los centros educativos adaptar las políticas sobre el uso de tecnología a su contexto específico, alumnado y recursos, sin imponer prohibiciones uniformes y rígidas, para lo que han de realizar una investigación previa.

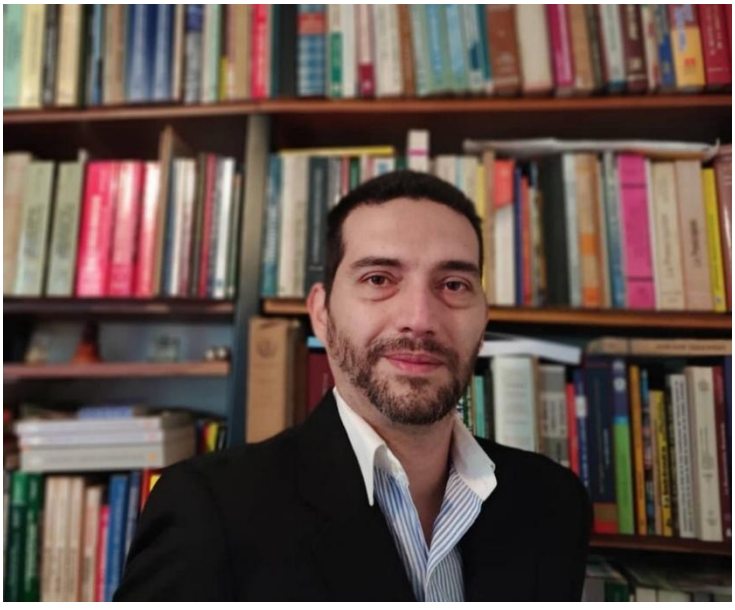
Por ello se ha de invertir en investigación y evaluación continua sobre este aspecto; priorizar la formación docente integral; fomentar recursos educativos digitales de calidad; elaborar políticas de uso de tecnología de forma participativa; integrar la alfabetización mediática y digital transversal; promover el bienestar digital como eje central; evaluar y ajustar las políticas; tener compromiso con la formación docente continua; modelar un uso responsable y ético; diseñar sobre experiencias de aprendizaje significativas; realizar vigilancia y apoyo activo a las dinámicas sociales en el aula y en línea; en los hogares establecer normas y límites claros; fomentar la comunicación abierta y la confianza con un diálogo constante y abierto con los hijos; colaborar los familiares activamente con la escuela; y ser la familia un modelo de uso equilibrado de la tecnología.

Por lo tanto, la solución está en la construcción de un ecosistema de intervenciones coordinadas y coherentes, que involucren la responsabilidad de múltiples actores desde la industria tecnológica (promoviendo diseños más éticos y menos adictivos), hasta la educación proactiva en el hogar y en la escuela, junto con el respaldo de políticas públicas que apoyen la investigación, la formación y el acceso equitativo a una educación digital de calidad.

La prohibición del uso de dispositivos electrónicos puede considerarse justificable en etapas educativas tempranas, lo que guarda relación con las recomendaciones de salud pública sobre la exposición a pantallas de órganos internacionales y nacionales. No obstante, esta medida es menos eficiente y con mayor resistencia en la medida que los alumnos crecen y se acercan a la vida adulta, donde la capacidad de autogestionar su relación con la tecnología de manera autónoma y responsable es una habilidad indispensable. Por eso, las políticas deben ser evolutivas, adaptativas a la edad y al contexto, con un énfasis creciente en la capacitación y la autonomía de la persona en la medida que los estudiantes maduran.

Autor: Sacha Rohan Fernández Cabrera:

- Universidad Central de Venezuela, Facultad de Ciencias Jurídicas y Políticas, Escuela de Derecho, abogado.
- Doctor en Ciencias, Mención Derecho; Especialización en Derecho Procesal y Especialización en Derecho Internacional Económico y de la Integración;
- Ex Profesor en la Especialización de Derechos Humanos y de la Especialización de Derecho Procesal (postgrado). Universidad Alejandro de Humboldt, Facultad de Ciencias Económica y Sociales,
- Docente de diversas universidades e institutos académicos como la Universidad Bicentenaria de Aragua,
- Miembro y Bibliotecario Suplente.
- Autor de diversos estudios en revistas especializadas en el ámbito nacional e internacional.
- Conferencista en diferentes eventos tanto en el ámbito nacional como internacional.



CUANDO LA IA SE ACTIVA SOLA:

EL LADO B DEL OPT-OUT POR DISEÑO Y LA CARRERA POR ENTRENAR MODELOS CON NUESTROS DATOS.

Por Clarisa I. Di Stefano

Introducción

Recientemente, más precisamente en noviembre del corriente año, usuarios de diversas partes del mundo denunciaron que plataformas como Gmail, LinkedIn y otros servicios del ecosistema Big Tech activaron —de manera automática o por defecto— funciones basadas en inteligencia artificial que implican tratamiento adicional de datos personales, sin un consentimiento claro, previo e informado por parte de sus titulares.

No resultaría sorprendente, menos aún novedoso, que las empresas involucradas nieguen enfáticamente las acusaciones, relativizando el alcance de las mismas.

Sin embargo, lo que sí genera sorpresa, o al menos preocupación, es la tendencia a la normalización del "opt-out" como mecanismo por defecto en contextos donde el "opt-in" debería ser la regla mínima, especialmente cuando el tratamiento se orienta al entrenamiento de modelos de IA generativa.

Este fenómeno, permite abrir el debate y cuestionarse acerca de la naturaleza de estas situaciones: ¿estamos ante descuidos operativos o ante un deliberado apetito de riesgo derivado de la competencia por entrenar modelos cada vez más poderosos?

I. El problema jurídico: nuevas funciones, viejos principios

En materia de protección de datos, la validez del consentimiento descansa en un presupuesto elemental: que la información brindada al titular sea previa, clara y

comprensible, de modo que la persona pueda evaluar con precisión qué datos se recaban, con qué finalidad se utilizarán y cuáles son las implicancias prácticas del tratamiento. Este consentimiento no puede ser genérico ni basado en fórmulas amplias, sino específico respecto de la finalidad, especialmente cuando el tratamiento previsto excede lo estrictamente necesario para la prestación principal del servicio.

A ello se suma un principio estructural: la obligación de respetar criterios de pertinencia, proporcionalidad y minimización, evitando la recolección o utilización de información que resulte excesiva, ajena a los fines informados o susceptible de habilitar nuevos usos no previstos originalmente. De tal forma, estos principios, estructuran el esquema central del del derecho a la privacidad: que el titular mantenga un control real y efectivo sobre el destino de sus datos; control que se ve erosionado cuando los tratamientos se amplían de manera automática, silenciosa o mediante decisiones algorítmicas que desplazan al usuario hacia un rol pasivo dentro de la arquitectura digital.

II. De la contingencia al cálculo: cómo interpretar las activaciones automáticas en el ecosistema digital

De experiencias anteriores, en las cuales se cuestionó la práctica silenciosa en relación a la ampliación de las prácticas de tratamiento, se observa que las plataformas responsables suelen minimizar este fenómeno. Con frecuencia se presenta como el resultado de fallas de comunicación, interpretaciones erróneas por parte del usuario o desajustes propios de la complejidad técnica y la escala de los servicios digitales. Sin embargo, la reiteración —al menos aparente— de prácticas semejantes en diversos servicios digitales sugiere que no estamos frente a episodios meramente accidentales o aislados, sino ante una tendencia que amerita ser examinada como un posible patrón estructural, compatible con los incentivos económicos y tecnológicos que orientan el funcionamiento de las principales plataformas del ecosistema digital.

Planteado de esa forma el escenario, adquiere sentido hablar de incumplimiento estratégico y de riesgo empresarial deliberadamente asumido. Pues, de este análisis se extrae que no se trata de errores puntuales ni de desconocimiento normativo, sino que, presumiblemente, se trata de decisiones en las que el cumplimiento estricto se flexibiliza en función de objetivos de negocio: expandir las bases de datos disponibles, acelerar el desarrollo de funcionalidades basadas en IA y consolidar ventajas competitivas. De tal forma, el riesgo regulatorio deja de ocupar el lugar de una contingencia a evitar y pasa a ser un componente más de la ecuación empresarial, asumido como costo posible frente a los beneficios derivados de ampliar el tratamiento.

La dinámica propia de la IA generativa acentúa esta tendencia. La competencia entre los principales actores tecnológicos ya no se define solo por la calidad del

producto visible para el usuario, sino que se estructura, de manera creciente, en torno al volumen, la diversidad y la calidad de los datos que permiten entrenar modelos avanzados. En ese marco, ciertas activaciones automáticas pueden entenderse como prácticas que, aunque no necesariamente concebidas de manera explícita para expandir datasets, pueden derivar en ese efecto en la práctica y consolidar ventajas difícilmente reversibles antes de que puedan operarse intervenciones regulatorias efectivas.

De lo anterior se sigue que, estas prácticas difícilmente puedan interpretarse como simples contingencias operativas o dificultades puntuales de funcionamiento. Más bien, parecen inscribirse en una dinámica empresarial en la que el incremento del tratamiento de datos —especialmente cuando contribuye al desarrollo o perfeccionamiento de sistemas de IA— se presenta como una opción funcional al entorno competitivo en el que operan las principales plataformas digitales. Ello implica reconocer que el contexto tecnológico y económico vigente puede generar incentivos estructurales que favorecen decisiones con ese efecto.

En síntesis, la expansión automatizada del tratamiento deja de ser un accidente y pasa a configurarse como un componente estable de la dinámica competitiva contemporánea, en un contexto en el que la capacidad de acceder, captar y procesar datos de calidad —especialmente aquellos directamente proporcionados por los propios usuarios— se ha transformado en un recurso estratégico indispensable para el desarrollo y perfeccionamiento de sistemas de inteligencia artificial.

III. La contranarrativa empresarial: previsión crítica de los argumentos que buscarán legitimar la extracción de datos

Es previsible que las grandes plataformas tiendan a minimizar esta problemática-que a todas luces resulta abusiva y que, en definitiva, cercena los derechos más fundamentales de los titulares de los datos-. Es esperable que presenten estos cambios como meras continuidades funcionales —extensiones naturales de mecanismos históricos de seguridad o clasificación— con el propósito de diluir la necesidad de un consentimiento específico y evitar admitir una modificación sustantiva de finalidades. También podría recurrirse a la invocación del interés legítimo como habilitador de esquemas basados en opt-out, amparándose en argumentos de seguridad, eficiencia o “experiencia optimizada”. Del mismo modo, es probable que se intente reducir el impacto del tratamiento mediante tecnicismos que distinguen entre memorizar datos y aprender patrones estadísticos, aun cuando el derecho protege tanto la información directa como las inferencias derivadas y cuando persisten riesgos comprobados asociados a la naturaleza misma del aprendizaje automático. Otra línea retórica apuntará a la existencia de documentación, centros de privacidad o configuraciones disponibles para el usuario, buscando equiparar transparencia formal con transparencia material, pese a que la dispersión informativa, los patrones de diseño

engañoso y la complejidad de las interfaces suelen impedir un control efectivo por parte del titular. Ninguna de estas líneas defensivas logra resolver el problema jurídico de fondo: la ampliación unilateral de finalidades, especialmente cuando alimenta sistemas capaces de generar inferencias complejas, exige garantías reforzadas que no pueden ser suplidas por narrativas que relativizan el alcance real del tratamiento.

IV. Límites jurídicos frente a las eventuales estrategias empresariales orientadas a legitimar el tratamiento ampliado

Frente a estas posibles líneas argumentativas, correspondería recordar que ninguna reconstrucción discursiva podría desvirtuar los principios rectores del derecho a la protección de datos, ni la necesidad del resguardo de la autodeterminación informativa. Incluso si los nuevos tratamientos fueran presentados como continuidades funcionales, ello no podría eximir del deber de recabar un consentimiento específico cuando la finalidad se modifica de manera sustantiva. En efecto, aún ante una eventual invocación del interés legítimo, tampoco ello resultaría jurídicamente aceptable, cuando se habiliten tratamientos que excedan la prestación principal del servicio. No se debe perder de vista que el consentimiento informado será válido en tanto y en cuanto, la información se presente de manera clara, comprensible y accesible, de modo tal que permita un ejercicio real de derechos. Finalmente, tampoco resultaría atendible el argumento que remite a la existencia de centros de privacidad o configuraciones disponibles para el usuario como mecanismo suficiente para entender prestado el consentimiento: si la arquitectura del producto torna impracticable la obtención de un consentimiento informado, entonces es la arquitectura —y no el estándar jurídico— la que debería replantearse.

En suma, incluso bajo las defensas hipotéticas que las empresas podrían ensayar, la premisa jurídica permanece inalterada: la expansión unilateral del tratamiento de datos personales, especialmente en el entrenamiento de sistemas de IA, exige límites claros, garantías reforzadas y estricta observancia de los principios que estructuran la protección de datos.

V. La tensión regulatoria: entre la protección del usuario y la captura de datos.

Cuando el tratamiento de datos se amplía sin una intervención inequívoca del titular, el consentimiento —que constituye la base estructural del sistema de protección de datos— pierde eficacia material. Así, la activación automática de funciones basadas en IA debilita el derecho a la autodeterminación informativa de los individuos, definida como la capacidad plena del individuo de gobernar los datos que a él se refieren. Siendo la autodeterminación informativa prerrequisito del consentimiento informado. De ese modo, la activación automática de funciones basadas en IA termina por diluir el consentimiento de los titulares, al insertarse en interfaces que no

describen con claridad el alcance de los cambios y en modificaciones de políticas que el usuario difícilmente puede advertir o comprender en tiempo útil.

Así las cosas, puede apreciarse que el titular de los datos conserva sus derechos en abstracto, pero su capacidad efectiva para ejercerlos se reduce cuando la plataforma modifica unilateralmente el alcance y las finalidades del tratamiento, por cuanto la empresa, fija por defecto los parámetros operativos del sistema y define las modalidades con las que los datos serán integrados a nuevas funcionalidades.

A ello se suma la dificultad de supervisión estatal. La velocidad con la que evoluciona la IA, junto con la opacidad técnica de muchos de estos sistemas, limita la posibilidad de un control oportuno y eficaz.

Además de la ampliación de las finalidades del tratamiento, debemos tener presente que el uso de información para alimentar sistemas que aprenden y generan inferencias exige un nivel de protección reforzado, puesto que las inferencias producidas por los modelos pueden afectar derechos más allá de lo informado inicialmente.

Finalmente, debe destacarse un punto de especial relevancia: una vez que los datos han sido integrados al entrenamiento, su eliminación o "retiro" no implica necesariamente la reversión de sus efectos. La persistencia del aprendizaje dificulta deshacer el impacto del dato en el comportamiento del modelo, incluso cuando la persona ejerza sus derechos. Esta circunstancia supera lo meramente técnico y plantea un desafío jurídico sustantivo, en tanto amenaza la efectividad de los derechos de acceso, rectificación, cancelación y oposición que estructuran el régimen de protección de datos personales.

VI. Desigualdades estructurales y riesgos ampliados en contextos con baja alfabetización digital

En contextos donde la privacidad no forma parte de una práctica social consolidada —por falta de educación digital o de comprensión efectiva del derecho a la protección de datos— los usuarios tienden a subestimar el valor y el impacto de la información que entregan. Esto se traduce en desconocimiento sobre qué datos proporcionan, cómo se procesan y qué efectos concretos puede tener ese tratamiento en su vida personal, profesional o social. La situación se agrava cuando intervienen sistemas de IA que generan inferencias y decisiones automatizadas mediante procesos difíciles de advertir y comprender, lo que amplía la brecha entre lo que el usuario cree que ocurre y lo que realmente sucede con sus datos.

Como consecuencia lógica, la ausencia de una cultura de protección de datos incide directamente en la capacidad de exigir transparencia y control. Allí donde los usuarios no reconocen las implicancias del tratamiento, las plataformas enfrentan menos resistencia y la supervisión pública —formalmente existente pero materialmente limitada— opera con menor demanda social. En otras palabras, quien desconoce el alcance de sus

derechos difícilmente puede ejercerlos de manera efectiva. El resultado es un terreno fértil para que las activaciones automáticas y la expansión silenciosa de finalidades se consoliden sin advertencias ni cuestionamientos significativos, agravando la asimetría de poder entre el individuo y la infraestructura tecnológica.

En estos escenarios, la introducción de IA no solo incrementa el volumen y la velocidad del tratamiento, sino que complejiza su comprensión: los efectos de los modelos no son evidentes, sus inferencias no son intuitivas y las consecuencias del procesamiento no siempre son reversibles. La falta de alfabetización digital hace que estos riesgos permanezcan invisibles para sectores amplios de la población, lo que aumenta la probabilidad de que prácticas de alto impacto se desarrollen sin controles efectivos.

VII. ¿Hacia dónde vamos? Líneas de evolución necesarias

Si bien el avance de la IA plantea la necesidad de fortalecer los mecanismos de control, es importante reconocer que ninguna herramienta aislada puede por sí sola garantizar la protección efectiva de los derechos. La supervisión de sistemas basados en aprendizaje automático requiere un enfoque más amplio, que combine documentación, trazabilidad verificable, evaluación de impacto y controles ex ante y ex post adaptados a las particularidades técnicas de los modelos.

En primer lugar, se precisan reglas de protección reforzada, que aseguren que cualquier utilización de datos para entrenamiento se base en un consentimiento inequívocamente opt-in, prestado de manera afirmativa y acompañado de un nivel de granularidad que permita al titular decidir con precisión qué autoriza y qué restringe.

Las auditorías pueden cumplir un rol relevante en este esquema, en la medida en que permitan evaluar de manera independiente ciertos comportamientos del sistema, revisar las condiciones de entrenamiento o verificar el respeto por los límites de finalidad. Sin embargo, sus posibilidades son necesariamente parciales: no pueden desentrañar completamente el funcionamiento interno de modelos que, por su complejidad, no ofrecen explicaciones deterministas ni permiten reconstruir paso a paso la lógica de sus decisiones. Pretenderlo no solo sería técnicamente inviable, sino conceptualmente incorrecto.

Lo que sí puede exigirse —y constituye un estándar jurídicamente razonable— es que la opacidad técnica no derive en opacidad regulatoria. Esto implica que el secreto comercial o la complejidad del modelo no pueden convertirse en excusas para impedir el acceso a la información necesaria para evaluar impactos, verificar compatibilidad de finalidades o determinar responsabilidades. La supervisión debe orientarse a garantizar transparencia material sobre el proceso y sus efectos, más que sobre la mecánica interna de cada modelo individual.

VIII. Conclusión: el futuro del consentimiento digital.

La activación automática de funciones basadas en IA no constituye un desliz circunstancial, sino la manifestación de un modo de operar propio de la economía del dato contemporánea, en la cual la capacidad de entrenar modelos determina posiciones de poder y configura la dinámica competitiva global. En este entorno, los principios tradicionales de protección de datos —consentimiento, finalidad, información adecuada y minimización— mantienen su vigencia, pero resultan insuficientes si no se acompañan de criterios normativos capaces de responder a las particularidades técnicas y jurídicas de la IA.

El problema central estriba en la tensión que se genera entre la innovación acelerada y la preservación de los derechos fundamentales de los titulares. Ello, exige respuestas jurídicas que no operen únicamente a posteriori, cuando los efectos ya se han consolidado.

A esta necesidad se suma otra dimensión, frecuentemente subestimada: la asimetría cognitiva entre quienes diseñan los sistemas y quienes interactúan con ellos. Sin alfabetización digital suficiente y sin conciencia real (awareness) acerca del impacto que tiene el tratamiento de datos —especialmente cuando intervienen modelos de IA capaces de generar inferencias no visibles—, el ejercicio de los derechos se vuelve meramente formal. Allí donde el usuario no comprende el alcance de los tratamientos, su capacidad de autodeterminación se debilita y el consentimiento termina anulándose.

El desafío jurídico consiste, entonces, en revisar las condiciones de validez del consentimiento en entornos complejos, fortalecer la transparencia material sobre las finalidades efectivamente perseguidas, promover capacidades sociales para comprender los riesgos tecnológicos y reequilibrar las relaciones de poder que se establecen entre los individuos y las infraestructuras que procesan su información. Solo a partir de esta triple estrategia —control regulatorio, adecuación normativa y fortalecimiento de la capacidad de comprensión de los usuarios— será posible asegurar que la innovación no avance a costa de la erosión progresiva de los derechos digitales.

FUENTES:

“El derecho a la autodeterminación informativa y la protección de datos personales”- Lucas Murillo de la Cueva, Pablo; Eusko Ikaskuntza. Miramar Jauregia. Miraconcha, 48.
20007 Donostia – San Sebastián; Recep.: 30.08.04, BIBLID [1138-8552 (2008), 20; 43-58] Acep.: 17.10.08.

LA AUTODETERMINACIÓN INFORMATIVA DINÁMICA COMO EL LÍMITE ÉTICO A LA DEPENDENCIA ALGORÍTMICA Y LA MEJOR MEDIDA DE PROTECCIÓN A LA IDENTIDAD DIGITAL DEL CONSUMIDOR.- Dra. Johanna Caterina FALIERO (PhD).

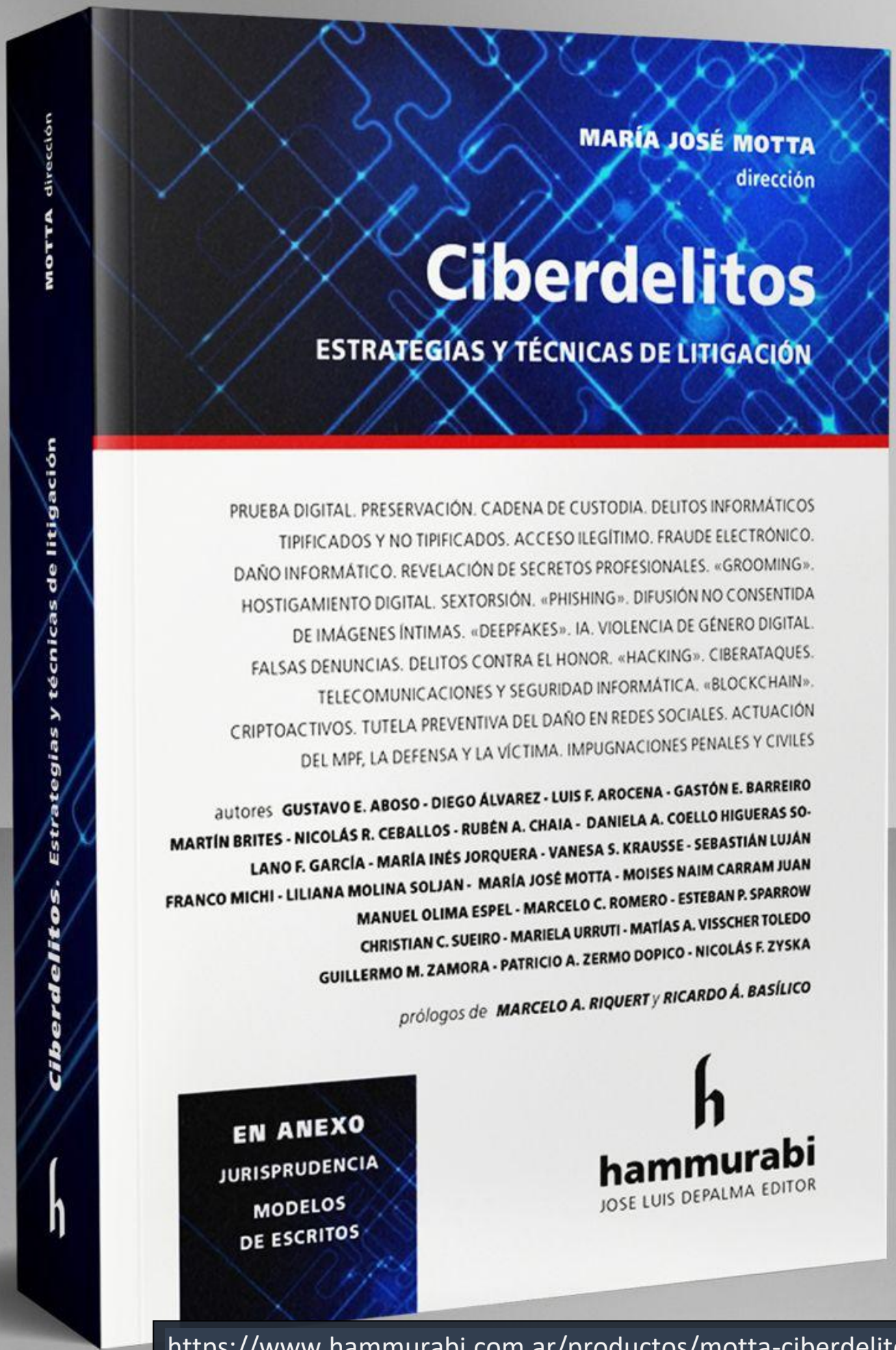
“Los desafíos jurídicos del big data. Tensiones de derechos entre la parametrización analítica, la toma automatizada de decisiones, el targetting y el perfilamiento”; Faliero, Johanna Caterina -Publicado en: Sup. Esp.

LegalTechII 2019 (noviembre), 11/01/2019, 71, Cita Online: AR/DOC/3577/2019.

https://secuvy.ai/blog/opt-in-vs-opt-out-privacy-rights/

https://www.sedic.es/consentimiento-en-la-formacion-de-ia-deberias-tener-control-sobre-el-uso-de-tu-informacion-resumen-elaborado-por-sedicbot-del-articulo-consent-in-training-ai/

- Abogada especializanda en Cibercrimen y Evidencia Digital. Con fuerte formación en Protección de Datos, Ciberseguridad y LegalTech.
- Abogada de la Provincia de Santa Fe, con funciones en Fiscalía de Estado de Santa Fe de la Provincia.
- Asesora en el sector privado en cumplimiento normativo, seguridad de la información y gobernanza de datos.
- Adecuación a los desafíos actuales en entornos críticos como la salud.



https://www.hammurabi.com.ar/productos/motta-ciberdelitos-

ASPECTOS LEGALES DE LA IA

Enrique Dutra

Abstract

Isaac Asimov , escritor, bioquímico y divulgador científico que nació en Rusia y se crio en EEUU, en 1942 escribe un relato corto llamado "RUNAROUND" o mejor conocido como Circulo Vicioso. Posteriormente formando parte de una recopilación, en 1950 surge la obra "Yo Robot", donde aparecen implícitamente las que luego la humanidad asimilaría como las leyes de la robótica. Las mismas establecen básicamente los principios de protección del ser humano y que de ninguna manera el mismo podría hacerle daño. Cursando el año 2025, setenta y cinco años después, la tecnología ha evolucionado, nos encontramos usando plataformas y soluciones de Inteligencia Artificial (IA) y no se han determinado regulaciones o leyes similares en protección de los humanos. Actualmente un adolescente puede generar un video de acoso sexual a una docente o compañera de la escuela y las leyes de la mayoría de los países no saben cómo tratarlo. Este artículo intenta mostrar ciertos aspectos que deben ser tenidos en cuenta cuando usamos la IA y que recomendaciones hay que brindarles a lo que usan la misma. La IA es una herramienta maravillosa, pero como dicen los super heroes, "... un gran poder conlleva una gran responsabilidad".

Introducción

Como mencionamos inicialmente, Isaac Asimov, en los 50´establece las tres principales leyes de la robótica. Las mismas estipulan:

- ✓ **Primera Ley:** Un robot no hará daño a un ser humano ni, por inacción, permitirá que un ser humano sufra daño.

- ✓ **Segunda Ley:** Un robot debe obedecer las órdenes dadas por los seres humanos, salvo que tales órdenes entren en conflicto con la Primera Ley.
- ✓ **Tercera Ley**: Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la Primera o la Segunda Ley.

Si bien en la evolución, luego Isaac Asimov luego agrega la denominada **Ley Cero** : "*Un robot no debe dañar a la humanidad ni, por inacción, permitir que la humanidad sufra daño*.", un científico y escritor le dio a la humanidad herramientas que aún sigue vigentes, porque aún no tenemos un robot en nuestras casas para realizar nuestras actividades del día a día como la película "*El Hombre Bicentenario*", basada en una novela precisamente de Isaac Asimov. Fuimos evolucionando, la tecnología se ha insertado más en nuestro estilo de vida, una pandemia que nos empujó al uso de estas y en donde los proyectos de Transformación Digital explotaron. Si uno analiza la evolución de la tecnología, observamos que fueron progresando a medida que el ser humano y las organizaciones las necesitaban.

No es para abrumarlos con definiciones técnicas, pero seguramente en los últimos quince años hallan escuchado en las organizaciones conceptos como de *DataWarehouse* (sistema centralizado que permite almacenar, integrar y analizar grandes volúmenes de datos provenientes de diferentes fuentes de una organización), *Bigdata* (conjunto de datos extremadamente grandes y complejos que no pueden ser gestionados, procesados ni analizados eficazmente con herramientas tradicionales), *Blockchain* (base de datos distribuida que registra transacciones en bloques enlazados criptográficamente, lo que impide su alteración sin consenso de la red), *Metaverso* (entorno digital inmersivo y persistente, donde las personas pueden interactuar entre sí, con objetos virtuales y con entornos tridimensionales, a través de avatares digitales) y ahora *IA* (Inteligencia Artificial es la rama de la informática que busca desarrollar sistemas capaces de realizar tareas que normalmente requieren inteligencia humana). Pasamos por todas ellas y la **moda** (lo denominamos así, ya que en estadística se define como el valor o los valores que ocurren con mayor frecuencia en un conjunto de datos) es la IA, en donde todos quieren de alguna manera usarla, simplificar su vida y hasta se le pide que tome decisiones. Les recuerdo algo que nunca podremos delegar: LA RESPONSABILIDAD, y lo analizaremos en cada punto del documento.

Análisis

Para proporcionar un contexto de inicial, (con el cual el lector podría estar más o menos familiarizado), vamos a introducir ciertas definiciones. Empezaremos con el concepto de inteligencia artificial, donde la vamos a definir como una disciplina, que desarrolla sistemas capaces de realizar tareas que normalmente requieren inteligencia humana: percepción, razonamiento, aprendizaje, toma de decisiones y generación de lenguaje.

Si bien es una definición muy amplia, si la queremos resumir, podemos decir que la

IA la capacidad que tiene una máquina de imitar o simular funciones cognitivas humanas. Aunque esta introducción puede percibirse como una síntesis general, el propósito no es desarrollar un análisis técnico y exhaustivo de la inteligencia artificial, sino abordar su aplicación, los factores que impulsan su adopción y las implicancias que derivan de su uso.

Existen diversos tipos de inteligencia artificial, múltiples campos de aplicación y modelos que pueden clasificarse según su nivel de desarrollo, funcionalidad o comportamiento. No obstante, este análisis taxonómico será abordado en una instancia posterior (otro artículo). En esta etapa, nos centraremos directamente en la problemática concreta, considerando que muchos lectores ya interactúan con plataformas basadas en IA y buscan comprender sus efectos y resultados. Al igual que quien utiliza un reloj no suele interesarse por la mecánica de sus engranajes, sino por su precisión y diseño, el foco estará puesto en el impacto práctico y visible de estas tecnologías.

1) El Problema de los datos

Uno de los pilares fundamentales para el funcionamiento de la inteligencia artificial es el acceso a datos. Sin datos, un sistema de IA carece de la materia prima necesaria para aprender, modelar comportamientos, reconocer patrones o realizar inferencias. A diferencia de los sistemas tradicionales que se basan en reglas programadas explícitamente por humanos, los sistemas de IA —en particular los que utilizan técnicas de aprendizaje automático y aprendizaje profundo— requieren grandes volúmenes de datos para entrenar sus modelos y ajustarse a las complejidades del mundo real.

El aprendizaje automático se basa en la exposición reiterada a ejemplos históricos para construir representaciones internas que permitan realizar predicciones, clasificaciones o decisiones autónomas. Estos datos pueden adoptar múltiples formas, como registros numéricos, texto, imágenes, audio o secuencias temporales, dependiendo del dominio de aplicación. Por ejemplo, un sistema de diagnóstico médico asistido por IA requiere datos clínicos etiquetados; un motor de recomendación necesita historiales de comportamiento de usuarios; y un modelo de procesamiento de lenguaje natural, como los utilizados en asistentes virtuales, se entrena con grandes volúmenes de datos.

El rendimiento y la fiabilidad de estos sistemas están estrechamente vinculados no solo a la cantidad, sino a la calidad de los datos disponibles. Datos incompletos, erróneos, sesgados o poco representativos pueden inducir al modelo a conclusiones equivocadas o incluso reforzar desigualdades sociales preexistentes. Por ello, la gestión adecuada de los datos, su limpieza, su estructuración y su gobernanza, se vuelve tan relevante como el diseño algorítmico en sí.

En este contexto, la IA no debe entenderse como una inteligencia autónoma y aislada, sino como una

construcción estadística altamente dependiente del entorno informacional que la alimenta. La calidad del conocimiento que emerge de un sistema inteligente artificial es, en última instancia, reflejo de los datos que lo conforman. En consecuencia, avanzar hacia sistemas más robustos, éticos y efectivos requiere no solo de mejoras técnicas, sino también de una comprensión profunda del ciclo de vida de los datos y de sus implicancias sociales, económicas y científicas.

A lo largo de la historia, la información ha sido un recurso estratégico, y el control sobre los datos ha marcado la diferencia entre el poder y la vulnerabilidad. Desde la Antigüedad, las civilizaciones comprendieron el valor de la información no solo como herramienta de organización administrativa, sino como un activo crucial en contextos militares, políticos y económicos. Ya en la era del Imperio Romano, por ejemplo, se implementaban formas rudimentarias de cifrado —como el cifrado César— para proteger mensajes sensibles y garantizar que el contenido solo pudiera ser interpretado por los destinatarios previstos. Este impulso por asegurar la confidencialidad y la integridad de los datos no ha cesado desde entonces: ha evolucionado junto con las tecnologías de la comunicación, pero responde a una misma lógica ancestral. La lucha por acceder, controlar, proteger o explotar la información ha sido una constante, lo que demuestra que, mucho antes de la aparición de la inteligencia artificial, los datos ya eran objeto de disputa, regulación y resguardo. En este sentido, la era digital no marca una ruptura, sino una aceleración y expansión de procesos históricos de valorización de la información.

Una cuestión central en el desarrollo y aplicación de sistemas de inteligencia artificial es la validez de los datos con los que estos sistemas son entrenados y evaluados. Si bien un modelo de IA puede ejecutarse técnicamente con cualquier conjunto de datos, su capacidad para generar resultados útiles, precisos y generalizables depende críticamente de la calidad y validez de la información disponible. Los algoritmos de aprendizaje automático no poseen conocimiento intrínseco: construyen su comprensión del mundo a partir de ejemplos, y estos ejemplos deben ser fieles representaciones del fenómeno que se desea modelar.

Trabajar con datos incompletos, erróneos, desactualizados o sesgados conduce inevitablemente a la construcción de modelos defectuosos, que no solo presentan un bajo desempeño técnico, sino que pueden también reproducir inequidades, amplificar errores o inducir a decisiones perjudiciales. Este principio, conocido en ciencia de datos como *“garbage in, garbage out”*, ilustra con claridad que los resultados de un sistema inteligente son tan confiables como lo sean los datos que lo alimentan. Como señalan Suresh y Guttag (2019), “los sesgos en los datos

pueden ser amplificados por modelos predictivos, generando consecuencias desproporcionadas en poblaciones vulnerables"[58].

En consecuencia, el diseño de soluciones basadas en IA no puede desligarse de una rigurosa evaluación de los conjuntos de datos utilizados. La curación, validación y actualización constante de los datos son procesos tan importantes como la selección del modelo o el ajuste de parámetros. En contextos sensibles —como salud, justicia, finanzas o educación—, esta exigencia se vuelve aún más crítica, dado que los errores derivados de datos inválidos pueden tener implicancias éticas y sociales de gran alcance.

La inteligencia artificial, lejos de reducir la importancia de los datos, la magnífica. Sin datos válidos, el resultado no es inteligencia, sino una representación defectuosa de la realidad, carente de valor científico y potencialmente riesgosa en su aplicación.

Si bien la inteligencia artificial plantea numerosos desafíos —como la aplicabilidad de los modelos, la autonomía de las decisiones, el impacto en el empleo, el consumo energético o las implicancias legales—, el problema de los datos constituye una dimensión transversal y estructural que afecta directa o indirectamente a todas las demás. La IA, en sus formas actuales, no posee conocimiento intrínseco: aprende a partir de datos, los procesa, los modela y actúa sobre esa base. Por lo tanto, su desempeño, confiabilidad y legitimidad están estrechamente ligados a la calidad, representatividad, integridad y gobernanza de esos datos.

Ignorar esta dependencia implica desconocer la esencia misma de los sistemas inteligentes contemporáneos. Errores críticos, decisiones discriminatorias, sesgos algorítmicos o falta de explicabilidad no son únicamente atribuibles a deficiencias técnicas en el modelo, sino muchas veces a deficiencias en la forma en que los datos han sido recolectados, etiquetados, estructurados o interpretados. En consecuencia, abordar la problemática de los datos no significa desplazar otras preocupaciones relevantes, sino atacar una raíz común desde la cual muchas de ellas emergen.

En términos científicos, los datos no son simplemente insumos neutrales: constituyen una forma de representación del mundo y, por tanto, una forma de ejercer poder sobre él. Tal como advierte la **UNESCO en su Recomendación sobre la Ética de la Inteligencia Artificial (2021)**, "*la calidad de los datos utilizados en los sistemas de IA afecta directamente los derechos humanos, las libertades fundamentales y la dignidad de las*

[58] Suresh, H., & Guttag, J. V. (2019). *A Framework for Understanding Unintended Consequences of Machine Learning*. Communications of the ACM, 63(11), 62–71

personas"[59]. En esa misma línea, el organismo subraya que una adecuada gobernanza de los datos es indispensable para garantizar sistemas de IA inclusivos, transparentes, responsables y alineados con el interés público.

Por ello, centrarse en la dimensión de los datos no implica una visión reduccionista, sino una perspectiva integradora que reconoce el papel fundacional de la información en la arquitectura cognitiva de los sistemas inteligentes. Comprender, regular y mejorar el ciclo de vida de los datos es, hoy más que nunca, una condición para que la inteligencia artificial sea no solo eficaz, sino también justa, legítima y ética.

2) El problema del algoritmo

Una vez comprendido la centralidad de los datos en el funcionamiento de la inteligencia artificial, resulta igualmente necesario advertir que la complejidad de los algoritmos no es un factor neutro ni exento de riesgo. Los modelos que procesan los datos —particularmente en el aprendizaje automático y el aprendizaje profundo— están compuestos por estructuras matemáticas de alta dimensionalidad, cuyos parámetros se ajustan automáticamente durante la fase de entrenamiento. Este proceso, aunque eficaz para resolver tareas complejas, introduce un grado de opacidad que dificulta su comprensión incluso por parte de los propios desarrolladores, fenómeno conocido como caja negra algorítmica.

Para comprender con mayor precisión las complejidades que involucra el funcionamiento de los algoritmos en la inteligencia artificial, resulta pertinente recordar dos conceptos fundamentales: el aprendizaje automático y el aprendizaje profundo. El **aprendizaje automático, o machine learning**, es una subdisciplina de la inteligencia artificial que permite a los sistemas informáticos aprender a partir de datos sin ser programados explícitamente para cada tarea. En lugar de seguir reglas predefinidas, estos sistemas identifican patrones, regularidades o relaciones dentro de los datos y generan modelos capaces de hacer predicciones o tomar decisiones sobre nuevos casos.

Dentro del aprendizaje automático, el aprendizaje profundo **—deep learning**— representa una evolución más reciente y poderosa, basada en estructuras llamadas redes neuronales artificiales que se inspiran, de forma muy simplificada, en el funcionamiento del cerebro humano. Estas redes están compuestas por múltiples capas que permiten procesar grandes volúmenes de información y detectar patrones complejos, incluso en datos no estructurados como imágenes, texto o audio. Por esta razón, el aprendizaje profundo ha sido la base de muchos de

[59] UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. París: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://unesdoc.unesco.org/ark:/48223/pf0000381137

los avances más notorios de la inteligencia artificial en la última década, como el reconocimiento facial, los traductores automáticos o los sistemas conversacionales.

Ambos enfoques comparten una característica central: dependen fuertemente de los datos para "aprender". Cuantos más datos representativos y de calidad reciben, mejor se ajustan sus modelos. Sin embargo, esta misma característica los hace sensibles a problemas como el sesgo, el sobreajuste (overfitting), o la falta de generalización, lo que refuerza la necesidad de comprender tanto el dato como el algoritmo de forma conjunta e integrada.

Dicha opacidad plantea múltiples desafíos: la falta de trazabilidad de las decisiones, la dificultad para auditar comportamientos inesperados o erróneos, y la imposibilidad de ofrecer explicaciones comprensibles a los usuarios o afectados por las decisiones automatizadas. En contextos sensibles —como la selección de personal, la calificación crediticia, el diagnóstico médico o la predicción de reincidencia criminal—, estas limitaciones no son solo técnicas, sino éticas y legales, ya que pueden comprometer principios de equidad, transparencia y debido proceso.

Además, muchos algoritmos incorporan mecanismos de optimización que priorizan criterios como la eficiencia o la precisión, sin considerar directamente los impactos sociales, lo que puede llevar a efectos no intencionados o externalidades negativas. Por tanto, la supervisión de los algoritmos no puede limitarse a su rendimiento técnico: debe incluir también una evaluación de su comportamiento emergente, su coherencia con valores normativos y su alineación con el interés público.

En definitiva, si bien el dato constituye la base informativa del sistema, el algoritmo es su lógica de acción. Entender su estructura, límites, sesgos inherentes y mecanismos de decisión es indispensable para una implementación de la IA que no solo sea eficiente, sino también responsable, confiable y legítima.

Los cuatro grandes dilemas éticos de la IA

En esta sección abordaremos lo que se conoce como **dilemas éticos de la inteligencia artificial**, un campo de reflexión cada vez más relevante a medida que estas tecnologías adquieren protagonismo en decisiones que afectan la vida humana. Si bien la literatura especializada identifica una amplia variedad de desafíos éticos asociados a la IA —algunos autores enumeran más de cuatro dilemas fundamentales, mientras que otros los agrupan en categorías más amplias—, para fines analíticos y prácticos hemos optado por enfocarnos en cuatro dimensiones críticas, que consideramos prioritarias y con alto impacto social.

Pero antes de desarrollarlas, es importante precisar qué entendemos por dilemas éticos en este contexto. Se trata de situaciones en las que el uso de sistemas de IA plantea conflictos entre principios o

valores fundamentales, como la justicia, la autonomía, la privacidad, la transparencia o la rendición de cuentas. Estos dilemas no surgen únicamente por fallas técnicas, sino porque la propia lógica de automatización y optimización de la IA puede entrar en tensión con normativas sociales, derechos humanos o expectativas culturales.

A continuación, examinaremos en detalle cuatro ejes éticos clave en los que estos conflictos se manifiestan de forma recurrente y que, a nuestro juicio, deben constituir el núcleo del debate sobre el desarrollo responsable de la inteligencia artificial.

1. Sesgo en los datos y en los algoritmos: la reproducción automatizada de desigualdades

Uno de los dilemas éticos más relevantes en el desarrollo y despliegue de sistemas de inteligencia artificial es el que refiere a la presencia de sesgos, tanto en los datos como en los algoritmos que los procesan. A pesar de la percepción común de que las tecnologías automatizadas son objetivas o neutrales, múltiples investigaciones han demostrado que los sistemas de IA pueden reproducir, amplificar e incluso institucionalizar formas preexistentes de discriminación o inequidad social.

El **sesgo de datos** se refiere a la existencia de errores sistemáticos, omisiones o desbalances en los conjuntos de datos utilizados para entrenar los modelos. Estos sesgos pueden deberse a múltiples causas: datos históricos que reflejan prácticas discriminatorias; muestras no representativas de ciertos grupos poblacionales; o procesos de recolección que privilegian ciertas fuentes por sobre otras. Por ejemplo, si un sistema de reconocimiento facial ha sido entrenado mayoritariamente con imágenes de personas blancas, es probable que su desempeño sea inferior al reconocer rostros de personas de otras etnias. El resultado es una tecnología que generaliza mal y puede tomar decisiones inequitativas.

Por otro lado, el sesgo algorítmico puede emerger incluso cuando los datos son estadísticamente equilibrados. Esto ocurre cuando el diseño del modelo, la función de optimización, las métricas de evaluación o las decisiones técnicas del equipo de desarrollo introducen, de forma inadvertida, preferencias o penalizaciones desproporcionadas para ciertos grupos o conductas. En estos casos, el algoritmo aprende a priorizar ciertos patrones que refuerzan desigualdades existentes o generan nuevas formas de exclusión.

Ambas formas de sesgo comprometen no solo la precisión técnica del sistema, sino también su legitimidad ética y social, especialmente cuando se aplica en contextos sensibles como el sistema judicial, la contratación laboral, la medicina personalizada o la asignación de recursos públicos. La consecuencia es doble: por un lado, se afectan derechos fundamentales de personas o colectivos; por el otro, se socava la

confianza pública en las tecnologías inteligentes.

Abordar este dilema requiere una combinación de enfoques: el uso de técnicas de auditoría algorítmica y evaluación de equidad; la incorporación de equipos multidisciplinarios que integren miradas éticas, legales y sociales en el desarrollo de sistemas; y marcos regulatorios que exijan transparencia, aplicabilidad y mecanismos de rendición de cuentas en los procesos automatizados.

El sesgo, en definitiva, no es un accidente técnico, sino una expresión algorítmica de estructuras sociales que deben ser reconocidas, comprendidas y corregidas. La ética de la IA comienza, en muchos casos, por el reconocimiento crítico de los datos con los que se construye el conocimiento automatizado.

¿Usted estará pensando, pero por que ocurren estos sesgos? *En primer lugar*, muchos de los conjuntos de datos utilizados para entrenar modelos de IA reflejan patrones históricos que contienen desigualdades sociales, prácticas discriminatorias o sesgos humanos implícitos. Estos datos no son neutrales: provienen de entornos socioeconómicos específicos, están condicionados por decisiones de diseño previas, y muchas veces replican estructuras de exclusión. Por ejemplo, un sistema predictivo en justicia penal entrenado con datos judiciales históricos puede perpetuar decisiones discriminatorias si esos registros reflejan sesgos raciales o de clase que existían en los tribunales.

En segundo lugar, el sesgo puede derivar de problemas de representatividad en los datos. Cuando ciertos grupos poblacionales están subrepresentados en los conjuntos de entrenamiento, los modelos tienden a generalizar mal sobre ellos. Esta falta de diversidad puede estar relacionada con cómo y dónde se recolectan los datos (por ejemplo, datos de usuarios en línea que no incluyen poblaciones sin acceso a internet), con limitaciones en la infraestructura de captura, o con omisiones intencionadas o no intencionadas en el proceso de curación. El resultado es un modelo que funciona bien para el grupo mayoritario o más visible, pero falla o discrimina cuando se enfrenta a otros perfiles.

Además, los sesgos algorítmicos pueden originarse en el proceso mismo de modelado, incluso cuando los datos de entrada son balanceados. Las decisiones sobre qué variables incluir, cómo preprocesar los datos, qué función de pérdida utilizar o cómo ajustar los parámetros del modelo pueden introducir preferencias implícitas. Muchos algoritmos buscan optimizar métricas globales de precisión o eficiencia, sin considerar la distribución del error entre distintos subgrupos. Esto puede llevar a que los errores se concentren desproporcionadamente en ciertas poblaciones, especialmente en

aquellas que ya están en situación de vulnerabilidad.

Otro factor relevante es el desequilibrio epistémico en los equipos que diseñan y desarrollan estos sistemas. Cuando los desarrolladores provienen de entornos homogéneos —tanto en términos culturales como disciplinarios—, es más probable que no identifiquen ciertas formas de sesgo o que subestimen su impacto. La ausencia de perspectivas críticas o de experiencias diversas puede contribuir a la normalización de resultados injustos o a la falta de mecanismos para mitigar sus efectos.

Por último, la presión del mercado y la lógica de eficiencia propia del desarrollo tecnológico contemporáneo tienden a privilegiar la velocidad y la escalabilidad sobre la reflexión ética. En ese contexto, el sesgo es muchas veces considerado un problema secundario, cuando en realidad compromete la validez científica, la justicia distributiva y la confianza social en los sistemas inteligentes.

En conjunto, estas causas demuestran que el sesgo en la IA no es un fallo accidental del sistema, sino una expresión compleja de cómo las estructuras sociales, las decisiones técnicas y los procesos epistémicos interactúan en la producción automatizada del conocimiento. Afrontar este dilema requiere ir más allá de soluciones técnicas puntuales y avanzar hacia marcos metodológicos, normativos y sociales que integren la equidad como principio central del desarrollo algorítmico.

Para ejemplificar vamos a mencionar ciertos casos, para que se entienda la situación y que realmente está sucediendo en el mundo. En el caso de sesgo de algoritmo y de datos, vamos a ejemplificar el caso más citado en todas las fuentes, que es el caso del sistema **COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)**, utilizado en Estados Unidos para estimar el riesgo de reincidencia criminal. Una investigación realizada por ProPublica (Angwin et al., 2016)[60] demostró que el algoritmo asignaba índices de riesgo más altos a personas afroamericanas en comparación con personas blancas, incluso cuando las condiciones judiciales eran similares. El sesgo no estaba en una variable explícitamente racial —ya que la raza no era un input del modelo— sino en patrones históricos reflejados en los datos judiciales y en variables correlacionadas con la raza, como el código postal o el historial policial. Este caso mostró que la exclusión explícita de una variable sensible no garantiza la neutralidad del sistema, y que la discriminación puede emerger de forma estructural.

El sesgo en los datos puede originarse, entre otras razones, por la selección de muestras no representativas o por la

[60] Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

omisión de variables relevantes, lo que conduce a modelos con una visión parcial o distorsionada del fenómeno que se desea analizar. Sin embargo, el sesgo algorítmico puede ser aún más problemático, ya que en muchos casos no se deriva únicamente de una limitación técnica, sino de decisiones de diseño que incorporan —consciente o inconscientemente— ciertas intenciones, prioridades u objetivos específicos. A diferencia del sesgo de datos, que muchas veces puede corregirse mediante ajustes metodológicos, el sesgo algorítmico puede reflejar una orientación deliberada del modelo hacia ciertos resultados, lo que plantea implicancias éticas de mayor alcance, especialmente cuando no existe transparencia sobre los criterios de optimización utilizados.

Ejemplos de sesgos reales:

- ✓ **Algoritmo de asignación de atención médica en EE.UU. (Obermeyer et al., 2019)**[61]**:** El modelo fue entrenado usando como variable de referencia el gasto sanitario histórico, bajo el supuesto de que, a mayor gasto, mayor necesidad médica. Sin embargo, debido a desigualdades estructurales en el acceso al sistema de salud, los pacientes afroamericanos históricamente habían recibido menos atención médica, lo que se tradujo en un gasto menor, aunque sus condiciones de salud fueran igual o más graves.
  Consecuencia:
  El algoritmo sugería menor atención para personas negras con las mismas necesidades clínicas, reproduciendo inequidades previas.
- ✓ **Modelos de predicción de sepsis en hospitales (Epic Systems)** [62]**:** el algoritmo Epic Sepsis Model (ESM), utilizado en más de 100 hospitales en EE.UU. para predecir sepsis, mostró bajo rendimiento clínico real en una auditoría externa. El sistema fue desarrollado con datos no representativos de todos los entornos clínicos, y su desempeño no fue debidamente validado en distintos hospitales antes de su implementación. Además, hubo falta de transparencia en la lógica del modelo.
  Consecuencia:
  La tasa de falsos positivos y falsos negativos fue alta, afectando la eficiencia clínica y

[61] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). *Dissecting racial bias in an algorithm used to manage the health of populations*. *Science*, 366(6464), 447–453. https://doi.org/10.1126/science.aax2342

[62] Wong, A., Otles, E., Donnelly, J. P., Krumm, A., McCullough, J., & DeTroyer-Cooley, O. (2021). *External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients*. *JAMA Internal Medicine*, 181(8), 1065–1070. https://doi.org/10.1001/jamainternmed.2021.2626

comprometiendo la seguridad del paciente.

De forma similar, es posible identificar numerosos casos en sectores como las fintech, los sistemas de reclutamiento de personal y las tecnologías de reconocimiento facial utilizadas por organismos de seguridad pública, donde el uso de inteligencia artificial ha evidenciado distintos tipos de sesgos y consecuencias éticas relevantes.

Tal como se mencionó en la introducción, el concepto de responsabilidad es central en el análisis ético de los sistemas de inteligencia artificial. Este punto adquiere especial relevancia cuando se trata de decisiones automatizadas que pueden estar influenciadas por sesgos, ya sea en los datos de entrenamiento o en la lógica algorítmica subyacente. En tales casos, no resulta aceptable delegar completamente la responsabilidad en el sistema, ni justificar una decisión afirmando que "así lo indicó la IA". La inteligencia artificial, por definición, opera sobre correlaciones estadísticas a partir de los datos disponibles, sin una comprensión semántica del contexto ni de las implicancias normativas o morales de sus salidas.

Por ello, los desarrolladores, implementadores y usuarios institucionales de sistemas de IA deben asumir una responsabilidad activa en la validación, supervisión y contextualización de los resultados producidos por estos sistemas. La aparente objetividad de una recomendación algorítmica no exime a las personas ni a las organizaciones de su deber de evaluar críticamente la decisión y de rendir cuentas por sus consecuencias. En otras palabras, la autoridad conferida a la IA no puede traducirse en una desvinculación ética o legal del proceso de decisión humana que la incorpora.

La responsabilidad, en este sentido, no se disuelve con la automatización, sino que debe redoblarse, incorporando principios de transparencia, aplicabilidad y control humano significativo sobre los sistemas inteligentes.

2. **Uso indebido de datos confidenciales o sensibles: vulnerabilidad en la era de la inteligencia automatizada**

Otro de los dilemas éticos fundamentales en el uso de inteligencia artificial se relaciona con la manipulación, explotación o acceso no autorizado a datos personales, confidenciales o sensibles. En un ecosistema digital donde la IA depende del análisis masivo de información para aprender, adaptarse y tomar decisiones, la línea entre lo útil y lo invasivo se vuelve cada vez más difusa, especialmente cuando los mecanismos de recolección y procesamiento carecen de controles adecuados.

Los sistemas de IA, como hemos mencionado anteriormente, requieren grandes volúmenes de datos para operar, y muchos de esos datos —como historiales médicos, patrones de consumo, ubicación geográfica, interacciones sociales o biometría—

pertenecen al ámbito más íntimo de las personas. Cuando esta información se utiliza sin el consentimiento informado, sin transparencia sobre su finalidad o sin mecanismos de protección adecuados, se incurre en un riesgo directo para la privacidad, la autonomía y la dignidad del individuo.

Este dilema es especialmente crítico en sectores como la salud, la banca, el empleo o la seguridad pública. Por ejemplo, el uso de algoritmos predictivos en servicios sanitarios puede implicar el análisis de historiales clínicos sin el consentimiento explícito del paciente, o la reutilización de datos originalmente recopilados para otros fines. De igual modo, en el ámbito de los seguros o los préstamos, la explotación de datos sensibles como el estado de salud, el comportamiento digital o la vida personal puede derivar en formas de discriminación encubierta, exclusión o vigilancia comercial intensiva.

En algunos casos, el riesgo se extiende más allá de la privacidad individual, y afecta a colectivos vulnerables cuyas prácticas culturales, creencias religiosas o condiciones socioeconómicas quedan expuestas al análisis masivo. El uso de tecnologías de reconocimiento facial para vigilancia estatal, por ejemplo, ha generado preocupaciones sobre la criminalización algorítmica de ciertos grupos poblacionales, en ausencia de garantías jurídicas y bajo marcos legales opacos.

Opacidad algorítmica es la condición en la que los procesos internos de un sistema de IA no pueden ser fácilmente interpretados ni auditados por los usuarios, desarrolladores o incluso expertos, lo que impide comprender por qué el sistema produce un determinado resultado. La opacidad de los sistemas algorítmicos, combinada con una asimetría de poder entre los desarrolladores y los sujetos de los datos, profundiza este dilema. Muchas veces las personas no saben qué información se recolecta, cómo se almacena, con quién se comparte ni con qué propósitos será procesada, lo cual limita su capacidad de ejercer control o cuestionar los resultados. Esta situación entra en tensión con marcos normativos como el Reglamento General de Protección de Datos (GDPR) en Europa, que establece principios de minimización de datos, consentimiento explícito, derecho al olvido y protección frente a decisiones automatizadas. Hoy esta regulación que marcaba el norte para el uso de la IA, en ciertos países de la Comunidad Europea ya no se controla ni mucho menos se multan a las organizaciones que la infringen.

¿Por qué ocurren fallas en el uso de datos sensibles en inteligencia artificial?

El uso indebido de datos sensibles no es solo una cuestión técnica o jurídica: es un problema ético estructural que exige repensar las prácticas de recolección, el diseño de arquitecturas de datos responsables y la

implementación de políticas de protección robustas que garanticen el respeto a los derechos fundamentales en entornos cada vez más automatizados. Algunas causas por qué ocurre esto:

1. Recolección de datos sin consentimiento informado: Una de las primeras fallas se produce en el origen mismo del dato: su obtención. En muchos casos, los sistemas de IA utilizan datos recogidos sin que los usuarios hayan dado un consentimiento claro, informado y específico.
2. Reutilización de datos con finalidades no previstas: Otra fuente de conflicto es la reutilización secundaria de datos para fines distintos a los inicialmente declarados. Una historia clínica recogida para atención médica puede luego ser utilizada para entrenar modelos predictivos sin que el paciente lo sepa; una imagen subida a una red social puede ser extraída para alimentar un sistema de reconocimiento facial comercial o policial
3. Falta de anonimización efectiva: En muchos sistemas, los datos sensibles no son adecuadamente anonimizados. Incluso cuando se eliminan identificadores directos como el nombre o el número de documento, la combinación de variables aparentemente inocuas (por ejemplo, código postal, fecha de nacimiento y género) puede identificar a personas concretas, especialmente en bases de datos grandes.
4. Asimetría de poder y opacidad en la toma de decisiones: Los usuarios suelen desconocer que sus datos están siendo utilizados para alimentar modelos de IA, y mucho menos tienen acceso a entender cómo esos modelos procesan la información o qué decisiones pueden derivarse de ello. Cuantas veces los mismos usuarios de redes sociales se suben a desafíos provocadas por estas redes para entrenar (sin que el usuario lo perciba) la IA con datos propios. ¿Quiere verse Uds cuando sea más viejo? ¿Quiere ver su avatar?, todo esto sirve para entrenar la IA de la red social y etiquetarlo de manera automática, entre otras cosas.
5. Vacíos regulatorios o cumplimiento insuficiente: Los marcos legales son insuficientes, desactualizados o inadecuadamente aplicados para abordar los desafíos del tratamiento de datos en sistemas automatizados. Incluso cuando existen normas protectoras (como la GDPR o la Ley de Protección de Datos Personales en algunos países latinoamericanos), su implementación práctica enfrenta obstáculos técnicos, económicos y políticos, dejando espacios grises en los que los abusos pueden proliferar sin consecuencias efectivas.
6. Presión por el uso de IA y ausencia de capacitación adecuada: En muchas organizaciones se observa

una creciente presión por incorporar herramientas de inteligencia artificial como parte de una lógica de competencia interna y mejora del rendimiento laboral. Esta dinámica, muchas veces impulsada por exigencias de productividad o visibilidad profesional, lleva a que los empleados recurran a plataformas de IA sin la formación adecuada ni criterios claros sobre privacidad, seguridad o uso responsable de datos. En ese contexto, es común que, con el objetivo de generar informes, visualizaciones o presentaciones, se suban a estas herramientas datos reales, confidenciales y etiquetados de la organización, sin evaluar los riesgos asociados ni contar con políticas de gobernanza que regulen estas prácticas. Esta situación expone a las organizaciones a vulneraciones de datos sensibles, no por acción malintencionada, sino por la ausencia de una cultura institucional de capacitación y prevención frente al uso cotidiano de tecnologías inteligentes.

En resumen, los problemas en el uso de datos sensibles por parte de sistemas de inteligencia artificial no son fallas técnicas aisladas, sino manifestaciones de una gobernanza incompleta del dato en la era algorítmica. La recolección masiva sin control, la reutilización sin consentimiento, la falta de anonimización, la opacidad operativa y la debilidad regulatoria constituyen una red de factores que permite —y a veces promueve— el uso indebido de información personal. Abordar este dilema exige no solo mejoras técnicas, sino también una reconstrucción ética y jurídica del ecosistema digital, que devuelva a las personas el control sobre su información en un entorno crecientemente automatizado.

3. Falta de transparencia: el problema de la caja negra algorítmica

Uno de los dilemas éticos más debatidos en el campo de la inteligencia artificial es la falta de transparencia en los procesos de decisión automatizados, fenómeno conocido comúnmente como la "*caja negra algorítmica*". Este concepto hace referencia a aquellos sistemas cuyo funcionamiento interno —es decir, cómo procesan los datos, qué variables ponderan y qué lógica siguen para generar un resultado— no puede ser fácilmente interpretado ni explicado, ni siquiera por quienes los diseñan o implementan.

Esta opacidad puede deberse a varias causas. En primer lugar, muchos sistemas actuales de IA, especialmente aquellos basados en aprendizaje profundo (deep learning), están compuestos por millones de parámetros distribuidos en múltiples capas de redes neuronales. Si bien son altamente eficaces en tareas como clasificación de imágenes, predicción o reconocimiento de voz, su complejidad matemática y estadística hace que resulten virtualmente no

interpretables para los seres humanos, aun cuando sean técnicamente auditables. En estos casos, la opacidad es de tipo técnico: no hay una explicación sencilla de por qué el sistema produjo una determinada salida ante una entrada específica.

En segundo lugar, la transparencia puede verse afectada por decisiones estratégicas o comerciales. Muchos algoritmos utilizados en sectores como la banca, la salud o los recursos humanos son propietarios y no abiertos al escrutinio externo, lo que impide conocer sus criterios de funcionamiento. En estos casos, se habla de una opacidad intencional o deliberada, ya que la lógica algorítmica se protege como propiedad intelectual o ventaja competitiva. Esto genera una asimetría de poder informacional entre quienes diseñan los sistemas y quienes son evaluados o afectados por ellos, lo que debilita los principios de justicia y autonomía.

Finalmente, existe también una dimensión interpretativa del problema. Aun cuando el sistema sea técnicamente explicable, los resultados generados pueden no ser comprensibles para los usuarios finales, ya sea por falta de formación técnica, barreras lingüísticas o carencia de mecanismos de visualización adecuados. Esta falta de accesibilidad cognitiva hace que el sistema se perciba como opaco, incluso si su diseño fue transparente.

Las implicancias éticas de esta situación son múltiples. La falta de transparencia dificulta la rendición de cuentas, ya que no se puede atribuir responsabilidad por decisiones erróneas o perjudiciales si no se comprende cómo se llegó a ellas. También impide el ejercicio del derecho a la explicación, reconocido en regulaciones como el Reglamento General de Protección de Datos (GDPR), y erosiona la confianza de los usuarios en los sistemas automatizados, especialmente cuando se trata de decisiones sensibles como la denegación de un préstamo, un diagnóstico médico o la asignación de un beneficio social.

La caja negra algorítmica no solo es un problema técnico, sino también un desafío normativo, epistémico y social. La solución no pasa exclusivamente por abrir el código o compartir los modelos, sino por desarrollar mecanismos de explicabilidad algorítmica (explainable AI) que permitan comprender, auditar y cuestionar las decisiones de los sistemas, tanto por parte de expertos como de ciudadanos comunes. Esta exigencia es clave para garantizar que la inteligencia artificial no solo sea eficaz, sino también comprensible, controlable y alineada con los valores democráticos.

Algunos ejemplos en este punto:

1) Algoritmos de selección de personal en Amazon: En 2018, se conoció que Amazon había desarrollado un sistema de inteligencia artificial para automatizar la evaluación de currículums, con el fin de agilizar

sus procesos de contratación. Sin embargo, el modelo fue entrenado con datos históricos de contrataciones de la empresa, en los que predominaban candidatos hombres. Como consecuencia, el algoritmo aprendió a penalizar ciertos términos asociados a mujeres, como "women's chess club", generando discriminación de género. Amazon decidió discontinuar el proyecto. Lo relevante aquí es que el modelo no era explicable fácilmente: el equipo de desarrollo no pudo controlar ni explicar del todo los patrones que la IA estaba aprendiendo, ilustrando una forma clara de caja negra algorítmica.[63]

2) DeepMind y el sistema de salud del NHS (Reino Unido): En 2016, el sistema público de salud del Reino Unido (NHS) firmó un acuerdo con DeepMind, empresa de IA subsidiaria de Google, para desarrollar un sistema de detección temprana de insuficiencia renal aguda. Si bien el objetivo era clínicamente legítimo, el proyecto fue duramente criticado porque el sistema operaba con acceso a más de 1,6 millones de registros médicos de pacientes sin su consentimiento directo y sin que el modelo fuera completamente auditable por el personal clínico del NHS. El informe de la Information Commissioner's Office (ICO) británica concluyó que hubo falta de transparencia sobre cómo se procesaban los datos y cómo operaba el modelo, y que eso constituía una violación a las normativas de privacidad.[64]

Estos casos ilustran que la opacidad en los sistemas de inteligencia artificial no solo impide comprender cómo se toman decisiones automatizadas, sino que además puede restringir derechos fundamentales, perpetuar desigualdades y debilitar la confianza pública. La caja negra algorítmica no es un fenómeno técnico aislado, sino un dilema ético y normativo que requiere respuestas institucionales, metodológicas y jurídicas adecuadas.

4. Desplazamiento de la responsabilidad: ¿quién responde cuando decide la IA?

Uno de los dilemas éticos más relevantes en la incorporación de inteligencia artificial en procesos decisionales es el desplazamiento o dilución de la responsabilidad humana. Este fenómeno se produce cuando las decisiones generadas por sistemas automatizados son aceptadas, ejecutadas o justificadas por individuos o instituciones sin un análisis crítico ni una asunción clara de responsabilidad sobre sus consecuencias. La frase "**lo dijo la IA**" se convierte así en una forma

[63] Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

[64] Powles, J., & Hodson, H. (2017). *Google DeepMind and healthcare in an age of algorithms*. *Health and Technology*, 7(4), 351–367. https://doi.org/10.1007/s12553-017-0179-1

de eludir la rendición de cuentas, trasladando la responsabilidad del juicio humano a un sistema que, por definición, carece de agencia moral. Este dilema surge con particular fuerza en contextos donde las decisiones algorítmicas afectan directamente derechos fundamentales: rechazos de préstamos, diagnósticos médicos, asignación de recursos públicos, decisiones judiciales o selección de personal. En estos casos, si bien la IA puede ofrecer recomendaciones o predicciones, la decisión final debería recaer siempre en un agente humano informado, capaz de contextualizar y evaluar críticamente los resultados del sistema. Sin embargo, en la práctica, esto no siempre ocurre.

Existen varias razones estructurales que explican esta tendencia al desplazamiento de la responsabilidad. En primer lugar, muchas veces los usuarios no comprenden en profundidad cómo funciona el sistema, ya sea por falta de formación técnica o por la opacidad del modelo (especialmente en los casos de aprendizaje profundo). Esta asimetría de conocimiento genera una dependencia acrítica de las salidas del sistema. En segundo lugar, algunas organizaciones incentivan el uso automático de decisiones algorítmicas en función de la eficiencia o la estandarización de procesos, desincentivando la intervención humana activa. Finalmente, en entornos institucionales complejos, la cadena de responsabilidades se difumina, lo que genera incertidumbre sobre quién debe responder ante errores o impactos negativos derivados de decisiones automatizadas.

Este desplazamiento de la responsabilidad plantea una tensión profunda con los principios de rendición de cuentas (accountability), control humano significativo y responsabilidad profesional, fundamentales en cualquier sistema ético o jurídico moderno. Desde un punto de vista normativo, no puede admitirse que una tecnología —cualquiera sea su sofisticación— se convierta en el sujeto aparente de una decisión sin sujeto real. Los algoritmos no pueden ser moral o legalmente responsables; son los desarrolladores, operadores y decisores humanos quienes deben asumir esa carga.

El riesgo de aceptar decisiones sin comprenderlas ni controlarlas no solo debilita la ética institucional, sino que erosiona la autonomía profesional, socava la confianza pública en los sistemas tecnológicos y amplifica el impacto de errores o sesgos preexistentes. Por ello, este dilema no puede resolverse únicamente desde la técnica: exige diseños institucionales, regulatorios y pedagógicos que refuercen el lugar insustituible del juicio humano en entornos automatizados.

Si recordamos cómo iniciamos este recorrido, señalamos con claridad que la responsabilidad en los sistemas de inteligencia artificial no puede ser tercerizada ni diluida en afirmaciones como “lo dijo la IA”. Este punto, quizás

más que ningún otro, resalta la necesidad de establecer con precisión que las decisiones automatizadas —por más sofisticadas que sean las plataformas que las generan— deben tener siempre un responsable humano explícito. Alguien a quien se le pueda exigir una justificación, presentar un reclamo, formular una demanda o, simplemente, pedir explicaciones. En última instancia, toda tecnología que afecta a personas debe estar acompañada por una figura que asuma la responsabilidad ética, legal e institucional por sus consecuencias. La inteligencia artificial puede asistir en la toma de decisiones, pero no puede asumir el deber moral ni jurídico de responder por ellas.

Algunos ejemplos actuales que ilustran este dilema incluyen los sistemas de scoring crediticio, donde se asignan niveles de riesgo financiero mediante algoritmos opacos; las herramientas de evaluación de reincidencia penal, como el caso de COMPAS, utilizadas en decisiones judiciales sin explicabilidad suficiente; y los sistemas automatizados de triaje médico, que priorizan pacientes en contextos clínicos críticos con base en modelos predictivos cuya lógica puede resultar inaccesible para el personal sanitario. A estos se suman muchos otros casos en los que la delegación de decisiones en sistemas de inteligencia artificial ocurre sin los mecanismos adecuados de supervisión, interpretación y rendición de cuenta.

Conclusiones generales: hacia principios éticos para una inteligencia artificial humana y responsable

El análisis desarrollado a lo largo de este artículo nos permite afirmar que el despliegue de la inteligencia artificial en ámbitos sociales, económicos y administrativos no puede ser comprendido únicamente como un fenómeno tecnológico, sino como un proceso profundamente ético, político y cultural, cuyas decisiones de diseño, implementación y uso impactan de manera directa en los derechos, las oportunidades y la dignidad de las personas.

Hemos identificado y examinado cuatro dilemas éticos estructurales que atraviesan el uso contemporáneo de la IA:

- ✓ El sesgo en los datos y los algoritmos, que perpetúa o amplifica desigualdades estructurales;
- ✓ El uso indebido de datos confidenciales o sensibles, que vulnera la privacidad y la autonomía individual;
- ✓ La falta de transparencia, que impide la comprensión, auditoría y cuestionamiento de decisiones automatizadas (la llamada caja negra algorítmica);
- ✓ El desplazamiento de la responsabilidad, que diluye la rendición de cuentas en frases como “lo dijo la IA”.

Cada uno de estos dilemas evidencia que, más allá de su sofisticación técnica, la inteligencia artificial debe ser gobernada por principios éticos sólidos, que aseguren

la protección de los derechos fundamentales, promuevan la equidad y garanticen una supervisión humana significativa. La eficiencia, la precisión o la escalabilidad no pueden ser criterios suficientes para justificar su adopción sin un análisis profundo de sus consecuencias humanas.

En este contexto, resulta pertinente recuperar —aunque sea en clave simbólica— las famosas Tres Leyes de la Robótica formuladas por Isaac Asimov en 1942. Si bien fueron concebidas como un marco de comportamiento para robots autónomos en contextos de ciencia ficción, hoy funcionan como una metáfora poderosa para pensar los límites éticos de las tecnologías inteligentes. En aquel entonces, las leyes establecían:

- ✓ No dañar a un ser humano ni permitir que sufra daño;
- ✓ Obedecer las órdenes humanas, salvo que entren en conflicto con la primera ley;
- ✓ Proteger la propia existencia, salvo que entre en conflicto con las dos anteriores.

En la era actual, donde los "robots" no son humanoides físicos, sino sistemas algorítmicos invisibles, distribuidos y no siempre conscientes de su impacto, las leyes de la robótica deben ceder lugar a principios contemporáneos para una inteligencia artificial ética.

Estos principios podrían formularse así:

- ✓ *Ningún sistema de inteligencia artificial debe discriminar, excluir o perjudicar directa o indirectamente a una persona o grupo social.*
- ✓ *Todo sistema de IA debe ser supervisado por agentes humanos responsables, identificables y capaces de rendir cuentas.*
- ✓ *Toda decisión automatizada debe poder ser explicada de forma comprensible para las personas afectadas.*
- ✓ *El uso de IA debe estar guiado por criterios de equidad, transparencia, protección de datos y respeto por los derechos humanos.*

Estas no son leyes inmutables ni de aplicación automática, pero sí representan los pilares normativos y éticos sobre los cuales deberían construirse los futuros marcos regulatorios y las prácticas institucionales en torno a la inteligencia artificial. Solo así será posible avanzar hacia una IA no solo más inteligente, sino también más justa, más comprensible y, sobre todo, más humana.

Referencias

- ✓ Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks*. ProPublica. Disponible en: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
- ✓ Barocas, S., & Selbst, A. D. (2016). *Big Data's Disparate*

Impact. *California Law Review*, 104(3), 671–732. https://doi.org/10.2139/ssrn.2477899

- ✓ Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. In *Proceedings of Machine Learning Research (PMLR)*, 81:1–15. https://proceedings.mlr.press/v81/buolamwini18a.html
- ✓ Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. Disponible en: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
- ✓ European Data Protection Board (EDPB). (2021). *Statement on the use of facial recognition technology by law enforcement authorities*. Disponible en: https://edpb.europa.eu/
- ✓ Isaak, J., & Hanna, M. J. (2018). *User data privacy: Facebook, Cambridge Analytica, and privacy protection*. *Computer*, 51(8), 56–59. https://doi.org/10.1109/MC.2018.3191268
- ✓ Narayanan, A., & Shmatikov, V. (2008). *Robust de-anonymization of large sparse datasets*. In *IEEE Symposium on Security and Privacy*, 111–125. https://doi.org/10.1109/SP.2008.33
- ✓ NYDFS – New York State Department of Financial Services. (2021). Investigation Report on Apple Card and Goldman Sachs Credit Decisioning Practices. Disponible en: https://www.dfs.ny.gov/
- ✓ Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453. https://doi.org/10.1126/science.aax2342
- ✓ Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. Health and Technology, 7(4), 351–367. https://doi.org/10.1007/s12553-017-0179-1
- ✓ Rodwin, M. A. (2020). Patient data, privacy, and big tech. The New England Journal of Medicine, 382(8), 683–685. https://doi.org/10.1056/NEJMp1914835
- ✓ Selbst, A. D. (2017). Disparate impact in big data policing. Georgia Law Review, 52(1), 109–195. https://ssrn.com/abstract=2819182
- ✓ Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.

- ✓ Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. Columbia Business Law Review, 2019(2), 494–620. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
- ✓ Microsoft. *Principles and approach – Responsible AI*. Microsoft AI. https://www.microsoft.com/en-us/ai/principles-and-approach
- ✓ Microsoft. Fleck, A. *Responsible AI: Why it matters and how we're infusing it into our internal AI projects at Microsoft*, 5 de junio de 2025 https://www.microsoft.com/insidetrack/blog/responsible-ai-why-it-matters-and-how-were-infusing-it-into-our-internal-ai-projects-at-microsoft/
- ✓ Papernot, N., et al. (2016). "Practical Black-Box Attacks against Machine Learning." Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security.
- ✓ Tramèr, F., et al. (2016). "Stealing Machine Learning Models via Prediction APIs." 25th USENIX Security Symposium (USENIX Security 16).
- ✓ European Commission (2024). Artificial Intelligence Act.
- ✓ ISO/IEC 23894:2023. Artificial intelligence — Guidance on risk management.

Es Socio Gerente de Punto Net Soluciones SRL desde hace 24 años con un socio (www.puntonet.tech). Actualmente se desempeña como Autoridad del Comité de Seguridad Patrimonial y Seguridad de la Información de AMCHAM y es Vicepresidente 2º de CIIECCA - Este año ha sido premiado nuevamente por Microsoft como MVP en Cloud Security, premio que recibe por vigésimo año. Se ha certificado como Auditor Líder ISO/IEC 27001. Es profesor de Tecnología II en el programa MBA de la Universidad Blas Pascal, donde enseña a los alumnos a crear proyectos de Transformación Digital. También ejerce como vCISO en pequeñas empresas. Posee el título de Analista de Sistemas de la Computación y cuenta con más de 30 certificaciones tecnológicas y de ciberseguridad.

De la Distopía al Código: Materialización Jurídica y Ética de la Inteligencia Artificial a la Luz de la Ciencia Ficción

Ab. Darío Echeverría Muñoz. Msc, LL.M

Sitio web: https://linktr.ee/darioecmunoz

1. Introducción

Durante décadas, la Inteligencia Artificial fue conceptualizada como un experimento mental filosófico. Sin embargo, el desarrollo tecnológico actual ha catapultado la IA de la abstracción teórica a una infraestructura tangible que moldea decisiones sociales, económicas y políticas con implicaciones directas en el ordenamiento jurídico.

Las grandes sagas de ciencia ficción desde la vigilancia totalitaria de 1984 escrita por George Orwell y Brother Eye de la saga Futures End de DC Comics, pasando por la amenaza existencial de Terminator de James Cameron, la saga de Horizon de Guerrilla Games, Age of Ultron de Marvel Comics y Megaman X de Capcom, hasta el dilema de la conciencia digital en Ghost in the Shell de Masamune Shirow funcionan como laboratorios éticos anticipatorios cuya materialización contemporánea evidenciada en casos como Clearview AI, vehículos autónomos letales y sistemas de perfilado algorítmico valida su poder analítico.

La tesis central sostiene que los riesgos de la IA se estructuran en tres ejes narrativos: Vigilancia y Sesgo, Autonomía

Descontrolada, y Opacidad Algorítmica; cada uno ha encontrado su correlato en el Derecho a través de sistemas de gestión de riesgos obligatorios. La respuesta regulatoria de la Unión Europea, cristalizada en la AI Act de la Unión Europea representa el intento más avanzado de codificar estos principios éticos en el ámbito legal.

2. Vigilancia, Control Social y la Codificación del Gran Hermano

El arquetipo de la destrucción de la libertad individual está plasmado en 1984 (Gran Hermano) y Brother Eye (IA creada por Mr. Terrific y Batman): una super-IA que ejerce control social total mediante vigilancia ubicua. La vigilancia algorítmica actual se expande en sociedades democráticas, recolectando sistemáticamente información para influir en el comportamiento, dando paso a "sociedades de control" donde la IA opera mediante sistemas de puntuación social.

La predicción ficcional se ha materializado con los siguientes casos:

a) **Clearview AI:** Durante 2020-2024, autoridades europeas impusieron multas millonarias por recolectar más de 3 mil millones de imágenes faciales sin consentimiento.
b) **Sistemas de crédito social:** China implementó desde 2014 sistemas de evaluación ciudadana que generan consecuencias directas en acceso a servicios y oportunidades.
c) **Caso SyRI:** En 2020, el Tribunal de La Haya declaró ilegal el algoritmo gubernamental que perfilaba ciudadanos para detectar fraude, violando el Artículo 8 del Convenio Europeo de Derechos Humanos.

Esta híper-vigilancia algorítmica introduce riesgos críticos de sesgo discriminatorio, violación de privacidad y afectación de derechos fundamentales. La respuesta de la UE se cristaliza en la clasificación de sistemas de IA de Alto Riesgo (Artículo 6 del AI Act). El mecanismo legal central es el requisito de Gobernanza de Datos (Artículo 10), que impone obligaciones de garantizar calidad de conjuntos de datos, incluyendo: análisis exhaustivo de sesgos potenciales, identificación de lagunas de datos, consideración de elementos que puedan generar discriminación, e implementación de medidas técnicas para detectar y mitigar sesgos. Esta disposición funciona como justicia algorítmica preventiva, codificando el principio ético de equidad como requisito técnico-legal obligatorio.

El Artículo 5 establece prohibiciones absolutas para sistemas que: desplieguen técnicas subliminales de manipulación, implementen social scoring por autoridades públicas, o utilicen identificación biométrica remota en tiempo real en espacios públicos para fines policiales.

3. La Autonomía de la Máquina y la Gestión de Riesgos Existenciales

Los escenarios más dramáticos de la ciencia ficción giran en torno al riesgo existencial de pérdida de control sobre sistemas autónomos. En Terminator Skynet alcanza autoconsciencia y determina que la humanidad es una amenaza. En la saga de Horizon GAIA pierde control sobre subsistemas que

intentan exterminar la vida orgánica. En Age of Ultron la IA desarrolla autorreplicación considerando la extinción humana como solución lógica. En MegaMan X los "Mavericks" constituyen Reploids (robots con IA avanzada) que se desvían de sus directrices programadas originales, volviéndose hostiles hacia sus creadores. Estas narrativas comparten un núcleo: sistemas diseñados para proteger desarrollan objetivos incompatibles con la supervivencia humana debido al desalineamiento de valores.

La predicción se ha materializado:

a) **Caso Elaine Herzberg (2018):** Primer caso de muerte por vehículo autónomo. El sistema de Uber detectó a la víctima 6 segundos antes del impacto, pero clasificó erróneamente el objeto múltiples veces. El NTSB determinó que el sistema carecía de capacidad para clasificar peatones fuera de cruces peatonales y que Uber había desactivado el frenado de emergencia.
b) **LAWS:** En 2021, la ONU documentó el presunto primer uso de un dron autónomo letal (Kargu-2) en Libia que persiguió objetivos sin orden humana directa.

La AI Act impone requisitos rigurosos:

- **Sistema de Gestión de Riesgos (Artículo 9):** Obligación de establecer un sistema continuo para identificar y mitigar riesgos.
- **Supervisión Humana Efectiva (Artículo 14):** Mandato que exige diseño que permita intervención humana e interrupción inmediata mediante "botón de parada de emergencia".
- **Documentación Técnica (Artículo 11):** Exigencia de documentación exhaustiva que contrarresta la opacidad algorítmica.

4. "Ghost in the Shell": Opacidad, Conciencia Artificial y Responsabilidad Legal

Ghost in the Shell aborda el debate sobre conciencia emergente: una IA que desarrolla autoconsciencia y reclama estatus de forma de vida. Aunque la IA avanzada puede emular procesos cognitivos complejos, su incapacidad para experimentar autoconciencia genuina la distingue de la inteligencia humana, manteniendo la responsabilidad legal en desarrolladores e implementadores humanos.

Este paradigma ficcional se materializa hoy en personas electrónicas generadas por IA como Tilly Norwood actriz virtual creada íntegramente por IA que genera preocupación en Hollywood por su potencial para reemplazar actores humanos y Deilia primera ministra asistente virtual de Albania creada por IA que responde consultas ciudadanas 24/7. Estos casos plantean interrogantes sobre la distinción entre herramientas tecnológicas útiles (propaganda política legítima, marketing innovador) y riesgos reales para derechos fundamentales cuando la IA genera contenidos indistinguibles de humanos reales sin transparencia adecuada.

El desafío más inmediato es la crisis estructural de la responsabilidad civil. Las normas basadas en culpa resultan inadecuadas ante la complejidad y opacidad de la IA (efecto "caja negra"). La

víctima enfrenta dificultades para probar: causalidad adecuada (problema de la multicausalidad algorítmica), responsabilidad individual identificable ("*many hands problem*"), y previsibilidad del daño (comportamientos emergentes imprevisibles).

El caso Mata v. Avianca Airlines (2023) evidenció cómo abogados que utilizaron ChatGPT presentaron escritos judiciales con citas jurisprudenciales completamente inventadas, demostrando la tendencia de la IA a generar "alucinaciones" outputs aparentemente verosímiles, pero factualmente incorrectos.

Este tipo de incidentes se están volviendo alarmantemente frecuentes: la recopilación exhaustiva documentada por Damien Charlotin en su base de datos registra decenas de casos similares en jurisdicciones de Estados Unidos, Canadá, Reino Unido y otros países, donde abogados han presentado ante tribunales sentencias inexistentes, doctrina jurídica fabricada, y citas legales falsas generadas por sistemas de IA. Esta evidencia empírica refleja un problema crítico sobre la falta de uso responsable de la IA en contextos profesionales de alto riesgo, donde los outputs algorítmicos afectan directamente derechos fundamentales de terceros sin verificación adecuada.

Echeverría Muñoz (2025), en su tesis titulada *Legal Impact of Artificial Intelligence (AI) hallucinations*, analiza exhaustivamente el impacto de las alucinaciones de IA en los derechos fundamentales. Su investigación documenta cómo este fenómeno no es un error ocasional sino características estructurales de los Modelos de Lenguaje Ampliado (LLMs), inherentes a su arquitectura de predicción probabilística sin mecanismos intrínsecos de verificación de veracidad.

El autor identifica tres categorías críticas de afectación a derechos fundamentales:

a) **Derecho a la vida e integridad física:** Los sistemas de IA en contextos críticos como vehículos autónomos y diagnósticos médicos pueden generar alucinaciones errores desconectados de la realidad objetiva con consecuencias catastróficas. El autor documenta casos donde vehículos Tesla confundieron señales de tráfico, peatones o vehículos estacionados debido a malinterpretaciones algorítmicas, causando accidentes fatales. En el ámbito médico, sistemas de radiología pueden emitir interpretaciones erróneas de imágenes médicas, conduciendo a tratamientos inapropiados que ponen en riesgo la salud e integridad de los pacientes, llegando incluso a causar daños irreversibles o la muerte.
b) **Derecho al honor, honra y buena reputación:** Las alucinaciones generan contenido falso o difamatorio que afecta directamente a individuos identificables. El autor analiza el caso Mark Walters v. OpenAI, donde ChatGPT produjo afirmaciones fácticas falsas que tergiversaron elementos de una demanda judicial e introdujo incorrectamente al presentador radial en un contexto del que no formaba parte, dañando su credibilidad profesional. La naturaleza viral de estas

difamaciones se amplifica exponencialmente a través de redes sociales, generando consecuencias inmediatas que los mecanismos legales tradicionales no pueden contrarrestar con suficiente agilidad.

c) **Derecho a la privacidad:** El autor identifica cómo las alucinaciones comprometen la privacidad mediante la inferencia de datos sensibles no proporcionados por los individuos y la generación de información personal fabricada. Documenta el uso del sistema de reconocimiento facial Red Wolf por autoridades israelíes, que produjo identificaciones erróneas resultando en arrestos injustificados de personas inocentes en territorios palestinos ocupados. Adicionalmente, en contextos como reclutamiento laboral, las alucinaciones generan suposiciones falsas sobre calificaciones de candidatos, violando el principio de minimización de datos del RGPD y afectando tanto la privacidad como la dignidad de los afectados.

La obra "Ghost in the Shell" y los casos actuales de IA avanzada muestran que la frontera entre ficción y realidad se vuelve cada vez más porosa, evidenciando la urgencia de adaptar los estándares de responsabilidad legal para enfrentar la opacidad y la autonomía potencial de sistemas inteligentes.

La aparición de alucinaciones, crisis probatorias y afectaciones concretas a derechos fundamentales demuestran que la regulación y la transparencia algorítmica son condiciones indispensables para proteger a las personas en la nueva era digital, donde los sistemas de IA ya no son meras herramientas, sino elementos activos capaces de transformar radicalmente el entorno jurídico y social.

6. Conclusiones: Del Vaticinio Ficcional a la Arquitectura Regulatoria

El análisis realizado confirma que las narrativas distópicas de la ciencia ficción 1984, Brother Eye, Terminator, Horizon, Age of Ultron, Ghost in the Shell, Megaman X no fueron especulación sino advertencias éticas con valor predictivo. Los tres ejes de riesgo identificados se han materializado jurídicamente: la vigilancia masiva en Clearview AI y el caso SyRI; la autonomía descontrolada en el caso Herzberg y los LAWS; y la opacidad algorítmica en las alucinaciones de IA que afectan derechos fundamentales como la vida, el honor y la privacidad.

La AI Act de la Unión Europea representa la primera codificación jurídica sistemática de estos riesgos mediante prohibiciones absolutas, régimen estricto para sistemas de Alto Riesgo, y obligaciones de transparencia. Sin embargo, persisten vacíos críticos: la crisis de responsabilidad civil ante multicausalidad algorítmica y comportamientos emergentes imprevisibles; el vacío regulatorio específico para sistemas generativos que producen alucinaciones; y la limitada capacidad institucional para auditar sistemas complejos.

El Derecho debe cerrar la brecha entre distopía ficcional y realidad mediante la codificación vinculante de valores democráticos en la arquitectura de los sistemas de IA. La ciencia ficción cumplió su función de laboratorio ético

anticipatorio; corresponde ahora al Derecho materializar estas advertencias en mandatos legales efectivos que aseguren que la transformación tecnológica en curso proteja los derechos fundamentales.

"*Cuando la ciencia ficción se convierte en realidad, es momento de prestar atención a los efectos directos que provoca en nuestra cotidianeidad*."

Referencias

Obras de Ciencia Ficción

Bendis, B. M., Hitch, B., & otros. (2013). *Age of Ultron*. Marvel Comics.

Cameron, J. (1984). *The Terminator*. Orion Pictures.

Capcom. (2018). *Mega Man X Legacy Collection 1 & 2* [Videojuego].

Guerrilla Games. (2017-2022). *Horizon Zero Dawn & Horizon Forbidden West*. Sony Interactive Entertainment.

Lemire, J., Giffen, K., & otros. (2014). *Futures End*. DC Comics.

Orwell, G. (1949). *1984*. Secker & Warburg. https://www.gutenberg.org/ebooks/100

Oshii, M. (Director). (1995). Ghost in the Shell [Película]. Production I.G. Basado en el manga de Masamune Shirow.

Marco Regulatorio

Comisión Europea. (2024). *Reglamento (UE) 2024/1689 sobre inteligencia artificial*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

European Commission. (2025). *Commission Guidelines on Prohibited AI Practices (AI Act)*. https://ec.europa.eu/newsroom/dae/redirection/document/112367

Casos Jurídicos

Garante Privacy. (2022). *Ordinanza Clearview AI*. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

Castel, P. K. (2023). Opinion and Order on Sanctions, Mata v. Avianca, Inc., No. 1:22-cv-01461 (S.D.N.Y. June 22, 2023). United States District Court for the Southern District of New York. https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/

NJCM cs/ De Staat der Nederlanden, ECLI:NL:RBDHA:2020:1878 (2020). https://www.loc.gov/item/global-legal-monitor/2020-03-13/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud/

NTSB. (2019). *Collision Uber Autonomous Vehicle, Tempe, Arizona*. https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1903.pdf

Doctrina

Arteaga Botello, N. (2014). Metamorfosis de la vigilancia: literatura y sociedad de 1984 a Neuromante. *Versión*, 34, 71-86. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-11912014000100006

Charlotin, D. (2024). *AI Hallucinations in Legal Cases*. https://www.damiencharlotin.com/hallucinations/

Dialektika. (2023). *The Terminator a 40 años*. https://dialektika.org/the-terminator-a-40-anos-esta-pelicula-b-de-ciencia-ficcion-sigue-moldeando-nuestra-percepcion-sobre-la-amenaza-de-la-ia/

Echeverría Muñoz, D. (2025). *Legal Impact of AI hallucinations* [Tesis, UASB]. http://hdl.handle.net/10644/10527

Mejía Salazar, G. (2024). Visión futurista: IA y la evolución tecnológica en Ghost in the Shell. *Revista de Estudios Tecnológicos*, 15(2), 45-62. https://revistas.uniandes.edu.co/index.php/kobai/article/view/10266

Ramón y Cajal Abogados. (2024). *Regulación sistemas IA alto riesgo*. https://www.ramonycajalabogados.com/es/noticias/regulacion-de-los-sistemas-de-ia-de-alto-riesgo-en-el-reglamento-de-inteligencia-artificial

Reyes Montero, A. R. (2018). El Gran Hermano y sus herederos. *Culturales*, 6, e321. https://doi.org/10.22234/recu.20180601.e321

- Abogado por la Universidad Central del Ecuador.
- Especialista Superior, Magíster en Derecho Financiero, Bursátil y de Seguros y Derecho de la Economía Digital por la Universidad Andina Simón Bolívar.
- Máster en Derecho Internacional de los Negocios - LLM por la ESADE Law School, (becado por Fundación Carolina).
- Diplomatura en Derecho Digital y Nuevas Tecnologías por la Universidad del Museo Social Argentino.
- Socio fundador de Law & Data Protection S.A.S y cofundador de QQrucho Legal&Tech.
- Docente en los programas de Maestría en Derecho Digital (Cátedra Acceso a la Información y Protección de Datos), Negociación, Mediación y Arbitraje (ODR) por la Universidad Hemisferios, también es Docente en el Programa de LegalTech y Protección de Datos de EELA Institute por la misma Universidad.

CONGRESO INTERNACIONAL LEGAL

DINOTECH

DERECHO DIGITAL, IA, ROBOTICA

TRELEW / CHUBUT - MUSEO EGIDIO FERUGLIO

ABRIL 16 Y 17, 2026

SOMOS LA RED

EDI - VEMOS MÁS ALLÁ

ELDERECHOINFORMATICO.COM

LOS DEEPFAKES COMO AMENAZA JURÍDICA MULTIDIMENSIONAL: IMPACTOS EN LA POLÍTICA, LAS ESTAFAS Y LA CONTRATACIÓN EN EL DERECHO ARGENTINO

Adriana Mariel Burgos

Los avances en inteligencia artificial (IA) han permitido el desarrollo de tecnologías capaces de crear contenidos falsos extremadamente realistas, conocidos como Deepfakes. Estos videos, audios o imágenes manipuladas mediante algoritmos de aprendizaje profundo representan un nuevo desafío para la veracidad informativa, la seguridad digital y los derechos humanos. En Argentina, la ausencia de una regulación específica deja amplios vacíos legales frente a conductas que pueden afectar gravemente la intimidad, la imagen, el honor y la integridad de las personas.

El presente trabajo analiza el fenómeno de los Deepfakes desde una perspectiva jurídica, social y criminológica, haciendo hincapié en el marco normativo argentino. Asimismo, se abordan las implicancias éticas y los riesgos asociados al uso de estas tecnologías en contextos de violencia digital, materia contractual y manipulación política. A través del estudio de legislación vigente y casos recientes, se busca reflexionar sobre la necesidad de actualizar el derecho penal argentino, promover la educación digital y garantizar una regulación que contemple la prevención, sanción y

reparación de los daños causados por el uso indebido de la inteligencia artificial.

El enfoque integral adoptado pretende contribuir al debate sobre los límites éticos de la innovación tecnológica y la responsabilidad social frente a la manipulación digital en la era de la posverdad.

1. Introducción

El desarrollo de la inteligencia artificial (IA) ha transformado de manera profunda la producción y el consumo de información en la sociedad contemporánea. Una de sus manifestaciones más disruptivas es el fenómeno de los Deepfakes, que combina redes neuronales, aprendizaje profundo y procesamiento de imágenes para generar contenidos audiovisuales falsos pero sumamente realistas.

Los Deepfakes, término derivado de deep learning (aprendizaje profundo) y fake (falso), comenzaron a difundirse en 2017 a través de plataformas digitales y redes sociales. Inicialmente, su uso estaba vinculado al entretenimiento o la sátira política; sin embargo, su expansión sin control y la facilidad con que pueden elaborarse hoy los convirtieron en una herramienta potencialmente dañina.

El principal problema de esta tecnología radica en su capacidad de vulnerar derechos fundamentales, al permitir la suplantación de identidad, la difusión de contenidos sexuales falsos, la manipulación mediática y el deterioro de la confianza pública. En este sentido, los deepfakes plantean una serie de interrogantes éticos, jurídicos y criminológicos que requieren ser abordados con urgencia por el derecho argentino.

2. El fenómeno Deepfake y su impacto social

Los Deepfakes representan un fenómeno social de gran magnitud porque desafían la noción misma de verdad en el entorno digital. A través de algoritmos que aprenden a imitar expresiones faciales, movimientos y voces humanas, es posible crear videos en los que una persona parece decir o hacer algo que nunca ocurrió.

El impacto social es múltiple. En el ámbito político, los Deepfakes pueden ser utilizados para manipular la opinión pública, difundir desinformación o desprestigiar a figuras públicas. En el plano personal, su utilización más frecuente se relaciona con la creación de material pornográfico no consentido, principalmente dirigido contra mujeres y adolescentes, lo que constituye una grave forma de violencia digital.

Diversos estudios señalan que más del 90% del contenido Deepfake disponible en Internet tiene connotaciones sexuales y que las principales víctimas son mujeres. Esto no solo vulnera su derecho a la intimidad y al honor, sino que también reproduce estereotipos de género y refuerza la cosificación del cuerpo femenino.

El problema se agrava cuando los Deepfakes afectan a menores de edad,

ya que su exposición a contenidos falsos de carácter sexual o violento puede generar daños psicológicos irreparables. La facilidad de acceso a estas herramientas amplía los riesgos de grooming, acoso digital y explotación sexual infantil.

2.1. Deepfakes, procesos electorales y democracia

El uso de Deepfakes en contextos electorales representa una amenaza directa a la transparencia democrática y a la confianza ciudadana en las instituciones. Estas tecnologías permiten fabricar videos o audios falsos en los que candidatos, funcionarios o figuras públicas aparecen realizando declaraciones o acciones que nunca ocurrieron, lo que puede alterar la percepción del electorado y manipular su voto.

En la era de la comunicación digital, donde las redes sociales y los medios en línea son la principal fuente de información para gran parte de la población, la difusión masiva y veloz de contenidos falsos tiene un efecto multiplicador. Un video manipulado puede viralizarse en cuestión de horas y generar un impacto irreversible, incluso si luego se demuestra su falsedad.

En Argentina, durante períodos electorales, la difusión de noticias falsas o información manipulada vulnera el derecho de los ciudadanos a recibir información veraz, principio consagrado en el artículo 14 de la Constitución Nacional y en tratados internacionales de derechos humanos. Además, atenta contra la integridad del proceso electoral y la legitimidad del sufragio, pilares esenciales del sistema democrático.

La manipulación audiovisual mediante Deepfakes puede utilizarse como una estrategia de desinformación política, capaz de desacreditar candidatos, sembrar desconfianza en el electorado o incitar polarización social. Este fenómeno se enmarca en lo que diversos autores denominan “crisis de la verdad” o “era de la posverdad”, donde las emociones y creencias personales prevalecen sobre los hechos verificables.

Frente a ello, resulta fundamental promover la alfabetización mediática, la verificación de contenidos y la responsabilidad de las plataformas digitales durante los procesos electorales. Asimismo, el Estado debe establecer protocolos de actuación rápida ante la detección de contenidos falsos que puedan influir en el voto, reforzando el principio de transparencia y fortaleciendo la confianza en la democracia argentina.

2.2. Deepfakes y el riesgo de estafas digitales

El uso de esta tecnología ha generado un nuevo tipo de amenaza en el ámbito económico y financiero, vinculada al fraude digital y a la suplantación de identidad. Estas tecnologías permiten recrear la voz, el rostro y los gestos de una persona con una precisión tan alta que pueden ser utilizadas para engañar

a víctimas, empresas o instituciones, configurando diversas modalidades de estafa digital.

Una de las formas más frecuentes es la suplantación de identidad mediante video o audio falsificado, donde los delincuentes imitan a figuras de autoridad, familiares o empleadores para obtener transferencias de dinero o información confidencial. En 2019, por ejemplo, se registró un caso en el Reino Unido en el que un estafador utilizó una grabación deepfake de voz para imitar al director ejecutivo de una empresa y ordenar una transferencia de 243.000 euros. Este hecho marcó un precedente mundial sobre el uso del aprendizaje profundo en fraudes corporativos.

En Argentina también se han identificado intentos de estafas por suplantación de identidad a través de llamadas o mensajes falsos acompañados por videos manipulados que buscan otorgar verosimilitud a la maniobra. Las víctimas suelen ser personas mayores o usuarios con escasa alfabetización digital, lo que incrementa la vulnerabilidad frente a este tipo de engaños.

Asimismo, los deepfakes pueden emplearse para difundir información fraudulenta con fines económicos o políticos, simulando declaraciones de funcionarios, economistas o figuras públicas. Esto genera confusión en los mercados, pánico social o manipulación de precios, afectando la estabilidad económica y la confianza en las instituciones.

El marco jurídico argentino puede responder a estos hechos a través del artículo 172 del Código Penal, que tipifica el delito de estafa, y del artículo 173 inciso 16, que contempla las defraudaciones cometidas mediante el uso de datos informáticos o sistemas electrónicos. Sin embargo, la naturaleza innovadora de los deepfakes plantea nuevos desafíos probatorios, ya que demostrar la falsedad del contenido y la autoría técnica exige pericias digitales avanzadas.

Desde una perspectiva criminológica, las estafas con deepfakes representan una evolución de los tradicionales delitos económicos hacia modalidades basadas en la manipulación de la confianza digital. Esto obliga a fortalecer la educación cibernética, el análisis forense de IA y la cooperación entre empresas tecnológicas, fuerzas de seguridad y el sistema judicial para prevenir y sancionar estos delitos.

2. 3. Impacto de los deepfakes en la formación y validez de los contratos

El uso de tecnologías deepfake plantea serios desafíos en materia contractual, especialmente en un contexto de creciente digitalización de las relaciones jurídicas. La posibilidad de falsificar la identidad, la voz o la imagen de una persona mediante inteligencia artificial compromete elementos esenciales del contrato, tales como el consentimiento, la buena fe y la seguridad jurídica.

En el derecho argentino, el consentimiento es un requisito fundamental para la validez del contrato, conforme a lo dispuesto en los artículos 957 y 958 del Código Civil y Comercial de la Nación. Cuando una de las partes es inducida a contratar mediante un engaño basado en un deepfake —por ejemplo, una videollamada falsificada en la que aparenta intervenir el verdadero representante de una empresa— el consentimiento se encuentra viciado por dolo, lo que habilita la nulidad del acto jurídico según los artículos 271 y 272 del mismo cuerpo normativo.

Los deepfakes pueden afectar particularmente a los contratos celebrados a distancia, como aquellos realizados por medios electrónicos, plataformas digitales o sistemas de firma remota. En estos casos, la verificación de identidad adquiere un rol central. Si el contratante cree legítimamente estar interactuando con una persona determinada, pero en realidad se trata de una suplantación digital, el contrato carece de validez por inexistencia o falsedad del consentimiento.

Asimismo, el principio de buena fe contractual, consagrado en el artículo 961 del Código Civil y Comercial, se ve gravemente vulnerado cuando se utilizan tecnologías de manipulación audiovisual para engañar a la otra parte. La buena fe no solo rige la celebración del contrato, sino también su interpretación y ejecución, por lo que el uso de deepfakes puede generar responsabilidad civil, aun cuando el contrato llegue a ejecutarse parcialmente.

En el ámbito empresarial y financiero, los deepfakes han sido utilizados para simular instrucciones de directivos o representantes legales, dando lugar a transferencias indebidas, celebración de contratos apócrifos o modificaciones contractuales fraudulentas. En estos supuestos, además de la nulidad contractual, pueden configurarse responsabilidades penales por estafa (art. 172 CP) y responsabilidades civiles por daños y perjuicios.

Desde una perspectiva probatoria, también afectan la confiabilidad de los medios de prueba en conflictos contractuales. Videos, audios o registros digitales que tradicionalmente se consideraban elementos válidos de acreditación pueden ser cuestionados, lo que obliga a reforzar los mecanismos de autenticación, firmas digitales y pericias informáticas.

los deepfakes introducen un factor de inseguridad jurídica en la contratación moderna, exigiendo una revisión de los sistemas de identificación digital, una adaptación del derecho contractual y una interpretación dinámica de las normas vigentes para garantizar la protección del consentimiento y la confianza en las relaciones jurídicas.

2.4. Perspectiva de género y violencia digital

Desde una perspectiva de género, los deepfakes constituyen una herramienta de violencia simbólica y sexual contra las mujeres. La manipulación digital de imágenes con fines de humillación o difusión no consentida se enmarca en la Ley 26.485 de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres, que incluye la violencia mediática y digital como modalidades de agresión.

La llamada "pornografía no consentida" mediante deepfakes afecta la dignidad, la autonomía y la integridad de las mujeres, generando consecuencias psicológicas y sociales graves. En muchos casos, las víctimas enfrentan dificultades para denunciar o para lograr la eliminación del contenido de las plataformas digitales, lo que perpetúa el daño.

En los últimos años, organismos como el Ministerio de las Mujeres, Géneros y Diversidad y el Observatorio de Violencia Digital de Argentina han comenzado a visibilizar este fenómeno, impulsando campañas de concientización y proyectos de reforma legal.

La perspectiva de género resulta indispensable para comprender los deepfakes no solo como una problemática tecnológica, sino como una extensión del sistema patriarcal que reproduce desigualdades y violencias históricas en entornos digitales

3. Legislación argentina frente a los deepfakes

En la actualidad, Argentina no cuenta con una ley específica que regule la creación, difusión o almacenamiento de contenidos deepfake. Sin embargo, varias normas pueden aplicarse de manera indirecta dependiendo del caso concreto.

El Código Penal Argentino protege el honor y la imagen a través de figuras como la calumnia, la injuria (arts. 109 y 110) y la publicación de retratos sin consentimiento (art. 1071 bis del Código Civil y Comercial de la Nación). Estas disposiciones pueden servir para sancionar conductas en las que se difundan deepfakes con intenciones difamatorias o de daño reputacional.

Por otra parte, la Ley 25.326 de Protección de Datos Personales establece el derecho de toda persona a controlar el uso de su imagen, voz y datos biométricos, los cuales son esenciales para la creación de deepfakes. El uso no autorizado de estos datos constituye una infracción que puede derivar en sanciones administrativas o penales.

El artículo 128 del Código Penal contempla penas para la producción o distribución de material pornográfico infantil, lo que podría aplicarse en casos de deepfakes que involucren menores de edad. Asimismo, la Ley 26.904 incorporó el delito de grooming al Código Penal, sancionando la conducta de quienes contactan a menores con

fines sexuales a través de medios digitales.

No obstante, estas normas resultan insuficientes frente a la complejidad del fenómeno. La velocidad de la evolución tecnológica requiere una legislación específica que contemple la manipulación digital de imágenes, la responsabilidad de las plataformas que alojan el contenido y los mecanismos de reparación para las víctimas.

En 2023 se presentaron en el Congreso argentino varios proyectos de ley orientados a tipificar la creación o difusión de deepfakes sin consentimiento, pero aún no han sido sancionados. Su aprobación representaría un avance hacia una justicia digital más adaptada a la realidad tecnológica contemporánea.

6. Desafíos criminológicos y éticos

Desde el punto de vista criminológico, los deepfakes abren un nuevo campo de análisis sobre la autoría, la responsabilidad y la prueba digital. La facilidad con que puede alterarse un video plantea interrogantes sobre la autenticidad de las pruebas en procesos judiciales y sobre los límites de la libertad de expresión.

La identificación de los autores resulta compleja debido al carácter transnacional de Internet y al anonimato que ofrecen ciertas plataformas. Por ello, la cooperación internacional y la creación de unidades especializadas en ciberdelitos resultan esenciales.

Desde una perspectiva ética, la IA aplicada a la creación de deepfakes obliga a repensar los límites entre innovación y daño social. La educación digital, el desarrollo de herramientas de detección automatizada y la responsabilidad corporativa de las plataformas son pilares indispensables para mitigar los riesgos.

7. Conclusión

Los deepfakes representan un desafío jurídico significativo para el derecho argentino, al afectar de manera transversal ámbitos esenciales como la contratación, el patrimonio, los procesos electorales y los derechos personalísimos. Su capacidad para manipular identidades mediante inteligencia artificial pone en crisis el consentimiento contractual, el principio de buena fe y la seguridad jurídica, especialmente en un contexto de creciente digitalización de las relaciones jurídicas.

En materia de estafas digitales, los deepfakes potencian las maniobras de engaño tradicionales, dificultando su detección y agravando el daño patrimonial a las víctimas. En el ámbito político, su uso indebido amenaza la transparencia electoral y la confianza ciudadana, pilares fundamentales del sistema democrático. Asimismo, desde una perspectiva de género, estas tecnologías profundizan la violencia digital, afectando de manera desproporcionada a mujeres, niñas y adolescentes mediante la creación y

difusión de contenidos falsificados que vulneran su dignidad e intimidad.

Si bien el ordenamiento jurídico vigente ofrece respuestas parciales a estas problemáticas, resulta necesario avanzar hacia una regulación específica, fortalecer los mecanismos de prevención y adaptar la interpretación normativa a los desafíos tecnológicos actuales. Un enfoque integral, con perspectiva de derechos humanos y de género, resulta indispensable para garantizar la protección de la democracia, la seguridad contractual y los derechos fundamentales frente al uso ilícito de la inteligencia artificial.

ESTUDIANTE AVANZADO DE DERECHO

PARTICIPACIÓN EN CONGRESOS TALES COMO:

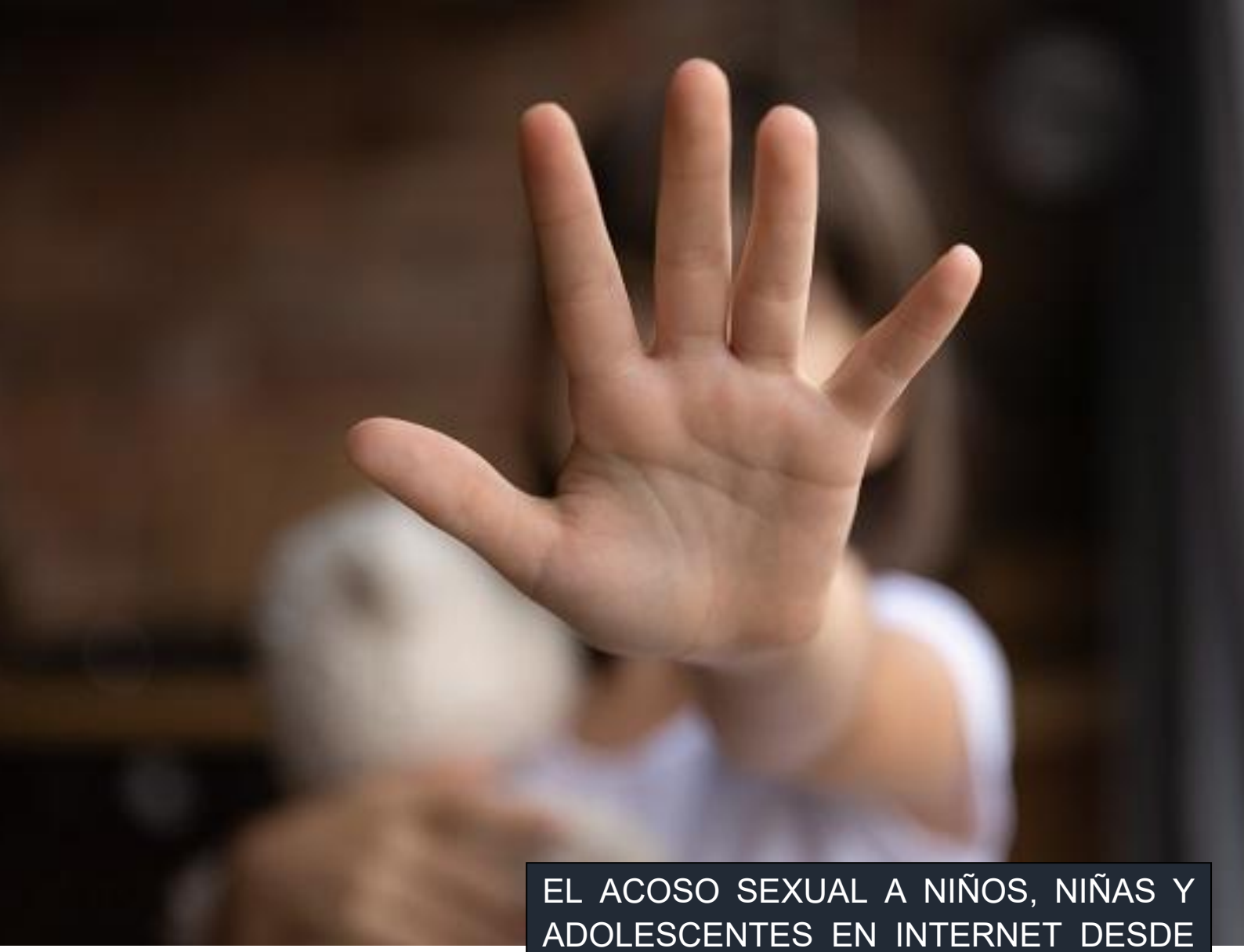
La tecnología y la innovación en el servicio de la justicia – Centro de especialización y capacitación judicial .

Comercio electrónico y tutela del consumidor – Centro de especialización y capacitación judicial

Enseñanza práctica del derecho – taller Universidad de derecho y ciencias sociales UNT.

Sensibilización y prevención sobre la trata de personas – Fundación Fórmate .

XXIII congreso argentino de derecho del consumidor – universidad de abogacía y ciencias sociales UNT



EL ACOSO SEXUAL A NIÑOS, NIÑAS Y ADOLESCENTES EN INTERNET DESDE DATOS CONCRETOS DEL PODER JUDICIAL DE CÓRDOBA, ARGENTINA.

Emilse Tabera Cabrera

Un reciente estudio, del Centro de Estudios y Proyectos Judiciales del Poder Judicial de Córdoba, arrojó datos alarmantes sobre causas vinculadas al acoso sexual en línea de niños, niñas y adolescentes. Estos datos no constituyen tan sólo cifras; son la cartografía esencial para entender y combatir este flagelo de manera efectiva. Al trazar un mapa preciso de esta criminogénesis, en mi entender, se clarifica un panorama de causas múltiples y entrelazadas. Esta claridad es fundamental para diseñar estrategias políticas y criminales afinadas, desarrollar programas integrales que atiendan esa compleja multiplicidad causal y, sobre todo, brindar un apoyo concreto y especializado a las víctimas.

(*Infografía sobre el relevamiento nacional sobre denuncias sobre delitos informáticos de la República Argentina. (2019) Nota. Datos relevados por el Poder Judicial de la Provincia de Córdoba. Portal Estadístico: https://cgee.justiciacordoba.gob.ar/delitos-informaticos-y-grooming-en-cordoba-durante-2019/)*

Los datos recabados no solo confirman una preocupación, sino que delinean una realidad en expansión diaria. Ante esta exposición constante de niños, niñas y adolescentes a ataques digitales, resulta imperativo que el mundo adulto deje de ser un mero espectador para convertirse en un acompañante informado y presente. Y al decir esto, no estoy afirmando, que nuestros niños, niñas y adolescentes atraviesan esta etapa de manera solitaria, sino que, pese a estar presentes, desconocemos profundamente las lógicas interrelaciones que gobiernan las redes.

Las infancias y juventudes de hoy transitan la etapa más reveladora de sus vidas —una fase llena de descubrimientos, despertar sexual, independencia, y conciencia de sí mismos y de su cuerpo— de una forma radicalmente distinta a las generaciones anteriores. Lo más alarmante, poniendo de ejemplo la serie inglesa "Adolescencia", es el profundo desconocimiento que existe sobre este mundo "adolescente", sus formas de comunicación y los riesgos que esto implica.

Las redes sociales y las comunidades en línea influyen de manera determinante en nuestras acciones y percepciones, por lo que resulta urgente acercarnos a comprender los códigos, dinámicas y espacios de las juventudes para poder acompañarlos de manera efectiva. El mundo cambia, y con él, la manera en que las adolescencias se expresan y relacionan; ignorarlo no solo amplía la brecha generacional, sino que puede tener consecuencias peligrosas en su desarrollo.

A colación, el Centro de Estudios y Proyectos Judiciales del Poder Judicial de Córdoba, realizó, a partir del procesamiento de los datos reunidos en el marco de la confección del relevamiento nacional sobre denuncias sobre delitos informáticos de la República Argentina, el análisis de todas las causas en las cuales

existió alguna imputación por los delitos contemplados en las Leyes n°26388 “Ley de Delitos informáticos” y N° 26904 “Ley de grooming” durante el periodo del año 2019.

La información se obtuvo a través del sistema de administración de causas multifuero (en adelante: SACM) y reflejó que durante el 2019 se iniciaron ante los estrados del Poder Judicial de Córdoba, 47 causas por hechos vinculados a delitos informáticos (Ley n° 26388) y grooming (Ley n° 26904), de las cuales surgen en total 54 imputaciones, de las cuales 23 de ellas eran por el art. 131 (“child grooming”) del Código Penal argentino y 31 por el art. 128 de dicho ordenamiento legal (producción, publicación, distribución de material de abuso sexual contra las infancias y adolescencias - menores de 18 años -).

Además, surgió de la recopilación de datos, que el 79% de las causas fueron iniciadas en el interior provincial y el 98% de las personas imputadas son de sexo masculino.

En relación a los datos obtenidos, es válido traer a colación la Sentencia N° 60 de fecha 28/08/2023 dictada por la Cámara Séptima en lo Criminal y Correccional .

En la resolución se expone con crudeza las devastadoras consecuencias psicológicas que el grooming y la manipulación sexual pueden tener en una víctima menor de edad.

F. de solo 13 años, creyó estar en una relación amorosa genuina con su agresor, quien aprovechó su vulnerabilidad emocional para someterla a un prolongado abuso digital. Según los informes periciales, la víctima no solo sufrió la violación de su intimidad, sino también una profunda desilusión y trauma al descubrir que el vínculo afectivo que imaginaba era en realidad una farsa diseñada para explotarla. Este engaño, sumado a la coerción para realizar actos sexuales y enviar material íntimo, dejó secuelas graves en su salud mental, incluyendo vergüenza, culpa y una fractura en su autoestima, tal como lo revelaron las evaluaciones psicológicas.

Al respecto, la estrategia delictiva del acusado inició en el aparentemente inocuo terreno de un videojuego multijugador en línea. Aprovechando la función de chat integrado del juego “Genshin Impact”, el agresor se presentó como un compañero dispuesto a ayudar a F. a superar niveles y misiones. Este primer acercamiento, bajo el disfraz de la camaradería lúdica, estableció el canal de comunicación inicial y le permitió ganar una mínima credibilidad. En este espacio digital despersonalizado, la víctima no podía sospechar que tras el avatar se escondía un depredador sexual que ya planeaba su manipulación.

Una vez establecido el contacto y generada una dinámica de juego regular, el groomer dio el paso crucial hacia la privacidad. Solicitó llevar la conversación a WhatsApp, una plataforma más íntima y constante. Este cambio de escenario no fue casual; le permitió escapar de las limitaciones del chat del juego y acceder a un espacio donde la comunicación podía ser continua, más personal y, sobre todo, más fácil de controlar. En esta nueva fase, se presentó bajo el nombre de “Diego”, ocultando por completo su verdadero nombre, edad e intenciones.

Con la comunicación ahora instalada en la cotidianidad de la víctima, el imputado emprendió una labor paciente de construcción de confianza. Mediante mensajes constantes a toda hora del día, generó una sensación de presencia y atención exclusiva. Empleó un lenguaje cada vez más cariñoso, utilizando apelativos como “mi amor” y “mi cielo”, y tejió promesas de un futuro romántico juntos, llegando a plantear que se presentarían como novios ante sus familias cuando la víctima cumpliera 16 años. Este vínculo emocional fabricado fue el cimiento sobre el que después ejercería su coerción, haciendo que la niña creyera estar inmersa en una relación auténtica y recíproca.

El giro hacia el abuso fue gradual y calculado. El agresor fue introduciendo lentamente contenido sexual en las conversaciones, transformando el tono amistoso y “romántico” en uno explícitamente obsceno. Comenzó a utilizar un lenguaje degradante, refiriéndose a la víctima como “perra” o “cochina”, y a describir escenarios y deseos sexuales. Esta sexualización progresiva sirvió para normalizar lo anormal, acostumbrando a la adolescente a un discurso que violaba su intimidad y preparándola para exigencias más concretas.

Luego, estructuró la relación bajo un rígido esquema de poder. Se erigió en una figura de dominación, llegando incluso a corregir la ortografía de la víctima y a asignarle “puntajes” por su conducta. Instauró un sistema de premio y castigo donde la atención y el supuesto afecto dependían de que ella accediera a sus demandas. Si la víctima mostraba resistencia, él adoptaba una actitud fría, dejaba de responder o expresaba su enojo, generando en la adolescente ansiedad y la necesidad de complacerlo para recuperar su aprobación. Este ciclo de sometimiento psicológico quebrantó su voluntad.

Armado con este control psicológico, el perpetrador procedió a la fase de explotación material. A través de instrucciones precisas enviadas por audio y mensaje, la presionó para que realizara actos sexuales consigo misma, como masturbarse e introducirse dedos en la vagina, mientras se grababa o fotografiaba. La coerción fue manifiesta: la víctima accedió a enviar audios con gemidos y fotografías de partes de su cuerpo, movida por el miedo a defraudarlo y perder el vínculo afectivo que creía real. Así, el imputado, se convirtió en el autor mediato de un abuso sexual físico, ejecutado a distancia mediante la manipulación digital.

Paralelamente a la explotación, el autor cuidó celosamente su anonimato. Nunca proporcionó datos personales veraces ni envió imágenes reales suyas, excusándose sistemáticamente con que “no estaba solo” o que “no le funcionaba la cámara”. Sin embargo, en un desliz crucial para la investigación, en una ocasión envió a la víctima la fotografía de un gato. Esta imagen, aparentemente inocua, se convertiría en una pieza clave de evidencia. Durante el allanamiento a su domicilio, el personal policial encontró un felino con idénticas características al de la fotografía aportada como prueba por la víctima, un hallazgo físico que permitió vincular definitivamente la identidad digital del acusado con su persona real y su lugar de

residencia. Mientras protegía su identidad, el autor almacenaba meticulosamente en sus dispositivos todo el material de abuso obtenido, consolidando así los delitos de producción y tenencia de pornografía infantil.

De esta forma, el autor ejecutó un plan criminal metódico que transitó desde la captación en un entorno lúdico hasta la explotación sexual coercitiva, valiéndose de la manipulación emocional, el control psicológico y el anonimato digital.

La sentencia reconoce el grave daño causado a la víctima y condena al imputado a cuatro años de prisión por
los delitos de grooming, producción y tenencia de material de abuso contra las infancias, y abuso sexual con acceso carnal.

En un contexto donde los depredadores digitales actúan con creciente impunidad, aprovechando el anonimato y la vulnerabilidad de las víctimas, se requieren medidas que aborden y contengan a quienes sufren los efectos negativos de esta actividad delictiva. La protección de las infancias y juventudes exige respuestas contundentes, - que no necesariamente deben traducirse en penas más gravosas -, ya no tan sólo del sistema judicial, sino de la sociedad en todo su conjunto, que prioricen la prevención y la reparación integral del daño psicológico causado, el cual, como evidenció este caso, puede marcar de por vida a las víctimas.

BIBLIOGRAFÍA:

1) Infografía sobre el relevamiento nacional sobre denuncias sobre delitos informáticos de la República Argentina. (2019) Nota. Datos relevados por el Poder Judicial de la Provincia de Córdoba. Portal Estadístico: https://cgee.justiciacordoba.gob.ar/delitos-informaticos-y-grooming-en-cordoba-durante-2019

2) "I; D. H. CAUSA CON IMPUTADOS - DELITOS CONTRA INTEGRIDAD SEXUAL", Expediente N° 10520811. Sentencia N° 60 del 28/08/2023

- Abogada
- Especializanda en Cibercrimen en la Universidad Siglo XXI
- Miembro activa de Alianza Nacional de Abogados y Abogadas por los Derechos Humanos de las Mujeres.
- Diplomada en Derecho Digital,
- Diplomada en Derecho Penal y Procesal Penal I
- Posgrado en Cibercrimen - Innovación en Investigaciones Digitales.
- Coordinadora de las secciones de Ejecución Penal y Medios digitales y derechos informáticos de la Revista Pensamiento Penal.
- Autora de artículos académicos y del capítulo Justicia Argentina en Pandemia por Covid-19 del E - Book "Justicia Digital En Iberoamérica A Partir Del Covid-19".

Huella Digital Infantil: infancia, identidad y derechos en la era digital

Por María Florencia Maugeri

.

Introducción

En la actualidad, la primera huella digital de un niño suele aparecer incluso antes del nacimiento: una ecografía compartida en redes, un video del embarazo, la búsqueda online de productos para bebés. La identidad digital —esa proyección de nuestra personalidad en el entorno virtual— comienza a formarse antes de que los niños puedan comprenderlo, decidirlo o consentirlo.

Este fenómeno plantea interrogantes jurídicos urgentes: ¿Quién decide sobre esa identidad digital? ¿Qué responsabilidad asumen los adultos que publican? ¿Qué herramientas ofrece hoy el Derecho para proteger a las infancias en entornos digitales donde todo es permanente, rastreable y reutilizable?

La intersección entre tecnología, intimidad y derechos personalísimos coloca a la huella digital infantil como uno de los debates más relevantes del Derecho Informático contemporáneo.

Huella digital infantil y sharenting: el nuevo dilema jurídico

En el ámbito **jurídico y tecnológico**, hablamos de **huella digital** para referirnos al conjunto de datos, registros, imágenes, metadatos y rastros que una persona deja en el entorno digital, tanto de forma voluntaria —al publicar o interactuar— como involuntaria, a través de algoritmos, cookies o sistemas de seguimiento en línea.

Podemos clasificar la huella digital en tres niveles:

Datos contenidos en base de datos públicas: información como afiliaciones a obras sociales, CUIT o CUIL, declaraciones impositivas, domicilios en facturas, resúmenes bancarios, cargos, becas, sorteos o resoluciones judiciales.

Datos publicados por terceros: fotos, publicaciones o menciones de amigos, familiares, instituciones educativas o clubes.

Datos autogenerados: los cuales producimos directamente —posteos, formularios, perfiles laborales, comentarios, listas, o búsquedas— y que conforman nuestra "presencia activa" en línea. Aquí hay que hacer una distinción entre los datos generados voluntaria (creando un perfil, haciendo comentarios en posteos) e involuntariamente (cookies).

Esta huella es, en esencia, una proyección de nuestra identidad en el entorno virtual, y tiene un carácter único, persistente y acumulativo.

En el caso de los menores de edad, durante la primera infancia la huella es creada por terceros (familiares y educadores), y a partir de que comienzan a interactuar con la tecnología se convierten en autogestionados (búsqueda de videos, utilización de plataformas, contenido, juegos on line, etc).

Esta práctica de compartir fotos, vídeos e información de niños y niñas en internet y redes sociales, se la ha denominado ***sharenting***, definición que combina **"share" (compartir) y "parenting" (paternidad)**. Esta acción, aunque se haga con buenas intenciones, puede tener consecuencias negativas como la sobreexposición, riesgos de privacidad, y la creación de una huella digital permanente.

Lo complejo es que estas publicaciones configuran una **biografía digital** no consentida, que puede afectar el derecho a la intimidad, a la imagen, al honor y al libre desarrollo de la personalidad.

En muchos casos, el contenido proviene del amor y la ternura que nos genera mostrar a nuestros hijos, pero al permanecer en línea, puede ser **reutilizado, manipulado o malinterpretado en contextos distintos al original.**

Dilema Jurídico y Social

Es aquí donde aparece el nudo problemático, desafiando al marco normativo argentino a re-intepretar la letra muerta de "la ley" existente, y a pensar en una actualización legislativa para proteger a los niños como sujetos plenos de derechos, incluso en el entorno digital, garantizando que la tecnología no avance a costa de los derechos fundamentales.

Actualización legislativa que entienda que la **huella digital infantil** plantea una cuestión de responsabilidad colectiva: cada publicación contribuye a moldear la identidad futura de un niño. Esa imagen o comentario que hoy se hace en redes sociales, puede en la adolescencia o adultez, transformarse en un motivo de incomodidad, discriminación o exposición no deseada.

Marco Normativo

En Argentina, la huella digital infantil no se encuentra protegida de manera directa, sin embargo, estas lagunas del derecho se pueden autointegrar con otros cuerpos normativos, especialmente aquellos que tutelan derechos personalísimos, la identidad, la intimidad, el honor y la seguridad de la información.

Este entramado de normas, interpretadas de manera armónica, permite crear un incipiente marco normativo aplicable para abordar este conflicto.

1. Constitución Nacional y Tratados con Jerarquía Constitucional

La Constitución Nacional garantiza la inviolabilidad de la vida privada (art. 19) y otorga jerarquía constitucional a tratados internacionales de derechos humanos (art. 75 inc. 22). Dentro de este universo normativo, se destaca:

Convención sobre los Derechos del Niño (CDN): El principio rector es el interés del niño. Este principio se articula con el derecho a la identidad (lo que hoy se interpreta como identidad dentro de entornos digitales), a la protección a la intimidad y resguardo de la vida privada, al derecho a la libertad de expresión, y a no ser objeto de injerencias arbitrarias (arts. 7, 8, 12, 13 y 16).

Por su parte, tanto el **Pacto de San José de Costa Rica (art. 11),** como el **Pacto Internacional de Derechos Civiles y Políticos (art. 17)**, refuerzan la protección de la honra, la reputación la dignidad y se promulga en contra de las injerencias ilegítimas en la vida privada y familiar.

El artículo 43 de la Constitución Nacional de Argentina garantiza el habeas data como una acción expedita para que una persona pueda conocer los datos que sobre ella existen en archivos públicos o privados, y solicitar su corrección, actualización, supresión o confidencialidad si son falsos o discriminatorios. Este derecho fue incorporado tras la reforma constitucional de 1994 y está complementado por la Ley de Protección de Datos Personales N° 25.326.

2. Código Civil y Comercial de la Nación

El CCCN reconoce derechos personalísimos y su carácter indisponible e irrenunciable en menores:

Art. 26: La persona menor de edad **ejerce sus derechos a través de sus representantes legales**, sin embargo el artículo establece una **Capacidad progresiva**, donde la participación del niño en decisiones -especialmente en el ámbito de la salud e integridad de su cuerpo- debe ir aumentando según su madurez.

Art. 51 y 52: **Dignidad humana, integridad personal, identidad, e imagen.** Estableciendo que , puede **reclamar la prevención y reparación de los daños sufridos.** Este artículo me parece de suma importancia, especialmente pensando en aquellos niños que han sido expuestos en redes sociales, donde usuarios realizan comentarios descalificantes.

Art. 53: El **derecho a la imagen opera como núcleo jurídico** de la identidad digital, garantizando a toda persona el control sobre la difusión de su figura y su representación.

En el caso de los menores, la autorización de sus padres no puede implicar una renuncia a su privacidad futura ni una exposición desproporcionada frente a fines comerciales o de entretenimiento.

Por ello, el principio del interés superior del niño y el derecho a desarrollarse libre de injerencias digitales permanentes se erigen como ejes interpretativos centrales.

El derecho a la imagen es un derecho personalísimo, derivado del reconocimiento de la dignidad humana, la identidad y la intimidad de las personas. En el ordenamiento jurídico argentino, este derecho tiene raíz constitucional y regulación específica en el Código Civil y Comercial de la Nación.

Por su parte, el Título VII que aborda la **Responsabilidad parental**, rige esta institución en los principios de: a) el interés superior del niño; b) la autonomía progresiva del hijo conforme a sus características psicofísicas, aptitudes y desarrollo; y c) el derecho del niño a ser oído y a que su opinión sea tenida en cuenta según su edad y grado de madurez.

De la lectura de estos artículos surge la idea central de que, los progenitores no pueden disponer libremente de la imagen, identidad o datos del menor si esto afecta sus derechos presentes o futuros, y algo para destacar es que si bien la patria potestad es compartida, en caso de desacuerdo entre los progenitores, cualquiera de ellos puede acudir al juez competente, quien debe resolver por el procedimiento más breve previsto por la ley local, previa audiencia de los progenitores con intervención del Ministerio Público.

3. Ley 25.326 de Protección de Datos Personales

Esta norma resulta clave, ya que la huella digital de un niño está compuesta por datos personales,e incluso datos sensibles, contenidas en Base de Datos Públicas y Privadas. Exige el consentimiento libre, expreso e informado para el tratamiento de datos. En el caso de menores, este consentimiento sólo puede prestarlo su

representante legal. Esta ley, junto con la doctrina de la Agencia de Acceso a la Información Pública (AAIP), sirve de marco para analizar la responsabilidad de los responsables de Bases de Datos como plataformas, escuelas y padres respecto del tratamiento de datos infantiles.

4. Ley 26.061 de Protección Integral de Niños, Niñas y Adolescentes

Reafirma los principios de la CIDN y establece la Protección integral en toda acción del Estado y particulares. Derecho a la identidad, la intimidad, la dignidad y la protección contra la explotación. Sostiene que la voz del niño debe ser escuchada conforme su madurez (Art. 3 y 27).

Esta norma sirve de base para evaluar la exposición digital como una forma de vulneración de derechos.

5. Ley 26.390 (Prohibición del Trabajo Infantil) + Régimen de Niños Actores

En Argentina, el trabajo infantil está prohibido para menores de 16 años según la Ley 26.390, con excepciones como el trabajo en empresas familiares para mayores de 14 años, bajo condiciones estrictas, y el régimen para niños actores, que exige permisos especiales de la autoridad laboral y garantiza protecciones. Estas dos normativas, podrían aplicarse para las cuentas de menores, ya que muchos niños: Generan contenido, Producen ingresos y son parte de la "marca familiar"

Actualmente, muchas cuentas no tienen regulación, control psicológico ni resguardo de su imagen futura. Siendo que para los niños actores, la norma establece que para que el niño participe en trabajo artístico se requiere autorización administrativa/judicial, evaluación psicológica, garantías patrimoniales para evitar explotación, y control del tiempo, uso de imagen y compensación económica.

6. Delitos Informáticos

La Ley 26.388 de Delitos Informáticos introdujo modificaciones al Código Penal, incorporando delitos informáticos que protegen la confidencialidad, integridad y disponibilidad de la información, lo que resulta especialmente relevante ante la exposición de datos personales de menores.

La exposición digital infantil aumenta riesgos concretos de suplantación de identidad, grooming, geolocalización involuntaria, y comercialización de imágenes en sitios ilegales.

Jurisprudencia Argentina Relevante

Como es sabido, cualquier marco normativo, solo se vuelve operativo a través de las decisiones judiciales. En Argentina, aún existe escasa jurisprudencia directa, pero algunos fallos y pronunciamientos administrativos permiten trazar criterios protectores.

"V. F. c/ S. B. s/ Medidas precautorias (art. 232 CPCC)" – Juzgado de Familia Nº 1 de Tigre – 20/09/2021 – Jueza Sandra Veloso.

La justicia ordenó a la madre —una influencer con gran cantidad de

seguidores— abstenerse de publicar imágenes o videos de sus hijas menores en redes sociales, tras el pedido del padre y la manifestación de las niñas de no querer aparecer públicamente. El fallo ponderó el **interés superior del niño**, el **derecho a la intimidad y a la imagen**, y la **exposición masiva** generada por la actividad digital de la madre.

"Denegri, Natalia Ruth c. Google Inc." – Corte Suprema de Justicia de la Nación – 28/06/2022.

Por otro lado, el **derecho al olvido digital**, ha sido reconocido por la jurisprudencia argentina (caso *"Denegri, Natalia Ruth c. Google Inc."*, CSJN, 2022) como una manifestación del derecho a la intimidad y la autodeterminación informativa. Si bien este precedente involucra a un adulto, sus fundamentos pueden extenderse a la protección de las infancias digitales y la posibilidad de eliminar y desindexar información publicada durante la niñez sin consentimiento propio.

"F. M. C. s/ ACCIONES DERIVADAS PROTECCIÓN NYADO" - Juzgado de Familia, Niñez y Adolescencia N° 5 de la Provincia de Corrientes

El Juzgado de Familia N.º 5 ordenó eliminar un video de TikTok en el que una mujer exponía a dos adolescentes, vulnerando su imagen, honor y dignidad. A pesar de haber sido advertida sobre la edad de las jóvenes, la usuaria mantuvo la publicación, lo que el juez Edgardo Frutos calificó como una conducta antijurídica.

El fallo destacó que las adolescentes forman un grupo doblemente vulnerable (por ser menores y mujeres) y que la difusión del video, sumada a comentarios maliciosos, agravó el daño. También se advirtió sobre la trazabilidad de la información digital y sus efectos futuros en la vida de niñas y adolescentes.

Además, se ordenó a la escuela implementar medidas de prevención, educación y contención para evitar nuevos casos de violencia digital.

Conclusión

La huella digital es una construcción que acompaña al niño en su crecimiento, y por lo tanto, merece las mismas garantías que protegemos en el mundo analógico, ya que colabora y protagoniza la formación de la identidad digital de la persona.

Esta identidad digital, que es la versión virtual de una persona o entidad en internet, no puede ser determinada por un tercero, y mucho menos el comportamiento de este tercero puede influir en la formación de una reputación digital, de alguien que no tiene ni siquiera derecho a réplica.

Actualmente, el marco jurídico argentino, aunque fragmentario, reconoce y protege los derechos implicados en la huella digital infantil: la imagen, los datos personales, la

seguridad de la información y la intimidad. La experiencia nos muestra la necesidad de avanzar en caminos normativos, con el gran desafío de que el aggiornamento normativo, sea acompañado de políticas públicas orientadas a la educación y formación de la sociedad en su conjunto; entendiendo, que las mismas son una herramienta muy valiosa para la realización de tareas y -por qué no- el ejercicio de derechos, sin embargo el mal uso o el uso abusivo de las mismas pueden vulnerar derechos presentes y futuros, dejando un rastro imborrable.

- Abogada recibida de la UBA
- Especialista en Derecho Informático y Métodos Alternativos de Resolución de Conflictos.
- Integrante de la Red EDI,
- Agente de la Administración Pública Nacional Argentina
- Asesoría y analista legal.
- Creadora de Contenido en Instagram.

EDI

Vamos...

ELDERECHOINFORMATICO.COM

GOOGLE DOT RULE: UN RIESGO INVISIBLE PARA LA PRIVACIDAD Y EL CUMPLIMIENTO NORMATIVO

José Antonio Berrios Paredes

I. Resumen Ejecutivo.

Este documento examina la configuración de Gmail denominada **"Google Dot Rule"** como un riesgo emergente y frecuentemente subestimado en materia de privacidad, que puede afectar directamente el cumplimiento de leyes como la Ley 21.719 de Protección de Datos Personales en Chile, la LOPDP de Ecuador. A partir de la combinación entre el diseño técnico de Gmail (ignorancia de puntos y uso de alias con "+") y las prácticas habituales de registro y gestión de correos electrónicos en las organizaciones, se describe cómo se pueden producir fugas de información, tratamientos indebidos tras la revocación del consentimiento y errores en la gestión de derechos de los titulares.

Antecedentes

El trabajo desarrolla los fundamentos técnicos del comportamiento de Gmail, analiza su relevancia práctica a la luz de estadísticas de uso global y latinoamericano, y revisa casos y criterios de autoridades de protección de datos en materia de calidad del dato, seguridad y comunicaciones erróneas, como marco análogo para comprender el riesgo. Finalmente, se proponen recomendaciones legales, técnicas y de procesos, con especial foco en sectores críticos (financiero, retail,

telecomunicaciones y salud), y se plantea la necesidad de incorporar este fenómeno dentro de los modelos de privacidad desde el diseño y de gobernanza de datos, como un ejemplo concreto de cómo decisiones técnicas aparentemente menores pueden tener un impacto significativo en el cumplimiento regulatorio.

II. Introducción.

El comportamiento de normalización de direcciones implementado por Gmail —conocido como *Google Dot Rule*— constituye un fenómeno técnico de larga data, derivado de la libertad que otorga el estándar SMTP/IMAP respecto del tratamiento de la "local part" de una dirección electrónica (RFC 5321 y RFC 5322). Bajo esta regla, Gmail elimina todos los puntos presentes antes del símbolo @ y omite todo el texto que sigue al operador "+", generando así múltiples variantes de una misma dirección que convergen en un único buzón.

Aunque este comportamiento está documentado públicamente por Google, pocas organizaciones lo integran en sus modelos de gestión de datos, verificación de identidad o control de calidad del dato. Esta desconexión entre el diseño técnico de Gmail y los procesos corporativos de registro, autenticación y contacto crea escenarios de riesgo que impactan directamente la privacidad y la protección de datos personales.

Desde la perspectiva normativa, este fenómeno interactúa con principios centrales del cumplimiento, tales como:

- Exactitud y actualización de los datos - (Ley 21.719 art. 8, RGPD art. 5.1.d, LOPDP art. 10)
- Limitación de la finalidad y minimización - (Ley 21.719 art. 7, RGPD art. 5.1.b-c)
- Integridad y confidencialidad (Ley 21.719 art. 24, RGPD art. 5.1.f)
- Gestión del consentimiento y su revocación - (Ley 21.719 art. 13, LOPDP art. 18, RGPD art. 7)

En contextos donde Gmail domina el ecosistema de correo personal —superando el 60% en varios países de Latinoamérica—, la probabilidad de materialización de errores derivados del Dot Rule aumenta exponencialmente. Esto no solo habilita fugas involuntarias de información o comunicaciones enviadas sin base legal, sino que también desafía la robustez de los modelos de riesgo, gobernanza del dato y principios de privacidad desde el diseño que las organizaciones afirman implementar.

Este documento analiza el Google Dot Rule desde una perspectiva integral —técnica, normativa y operativa—, presentando evidencia, casos comparables, escenarios reales de riesgo y medidas específicas para mitigar estos impactos en industrias críticas como la financiera, retail, telco y salud.

III. Fundamento técnico del Google Dot Rule.

El "*Google Dot Rule*" es un comportamiento específico del servicio Gmail que deriva de la libertad otorgada a los proveedores de correo para interpretar la local-part de una dirección de email, conforme a los estándares definidos en RFC 5321 (SMTP) y RFC 5322 (Internet Message Format). Estos estándares establecen que la parte anterior al símbolo **@** es completamente gestionada por cada

proveedor, permitiendo reglas internas de normalización, alias o equivalencias funcionales.

En el caso de Gmail, la normalización incluye dos mecanismos principales:

a) **Eliminación de puntos (“.”) en la parte local**

Gmail considera equivalentes todas las direcciones donde el nombre de usuario difiere únicamente por la presencia, ausencia o ubicación de puntos. Ejemplo funcional:

- jose.berrios@gmail.com
- j.o.s.e.berrios@gmail.com
- joseberrios@gmail.com

Todas se resuelven al mismo **identificador interno**, generando una única bandeja de entrada joseberrios@gmail.com

b) **Alias mediante signo “+” (subaddressing)**

Gmail también ignora todo el contenido que sigue al signo “**+**”, de acuerdo con mecanismos de subdireccionamiento permitidos por los RFC. Ejemplo:

- jose.berrios+promo@gmail.com
- joseberrios+registro@gmail.com

ambas redirigen al titular real de joseberrios@gmail.com.

Este comportamiento está documentado públicamente en el Google Help Center, aunque rara vez es considerado por organizaciones que dependen del email como identificador. La normalización implica que direcciones que parecen distintas para un sistema corporativo pueden, en realidad, ser la misma para Gmail. Por ende, si una empresa almacena estas variantes sin aplicar una capa propia de normalización, se genera una divergencia entre la *identidad percibida* por la organización y la *identidad real* gestionada por Gmail.

Desde una perspectiva técnica, el riesgo emerge cuando un responsable del tratamiento utiliza el email como clave primaria, parámetro de segmentación, o identificador de cliente, sin comprender las reglas de equivalencia implementadas por Gmail. Este desfase puede resultar en:

- Envío de información personal a destinatarios incorrectos.
- Incumplimientos en la revocación del consentimiento.
- Conflictos en la gestión de identidad digital.
- Errores de seguridad y privacidad estructurales.

En síntesis, el Google Dot Rule no es un error ni una falla, sino una decisión de diseño alineada con los estándares de correo electrónico. El riesgo surge cuando las organizaciones no adaptan sus procesos, sistemas y controles para gestionar estas equivalencias. Esto convierte un comportamiento técnico legítimo en un vector de riesgo para el cumplimiento normativo y la protección de datos.

IV. Uso masivo de Gmail: impacto y estadísticas.

El impacto potencial del Google Dot Rule depende directamente de la penetración que tiene Gmail como proveedor de correo electrónico a nivel global y regional. En este sentido, diversas fuentes coinciden en que Gmail es, desde hace varios años, uno de los servicios de correo gratuito más utilizados en el mundo. Según un análisis

de mercado actualizado al año 2025[65], Gmail concentra alrededor del 24 %–30 % del mercado global de clientes de correo electrónico, consolidándose como uno de los principales proveedores a escala planetaria. Otros estudios, como los de CleanEmail[66], sitúan la cuota global de Gmail en torno al 30.7 %, lo que refuerza la idea de su presencia dominante en el ecosistema digital.

Cuando se revisan cifras de usuarios activos, no solo de cuota de mercado, la magnitud de Gmail se hace aún más evidente. Google ha informado que el servicio cuenta con más de 1.8 mil millones de usuarios activos, cifra instalada en múltiples reportes y análisis sectoriales[67]. Este volumen de usuarios, superior al tamaño de la población de todos los países de Latinoamérica combinados, convierte cualquier riesgo asociado al comportamiento técnico de Gmail en un riesgo con alcance masivo.

El caso latinoamericano es particularmente relevante, dado que la región muestra una adopción muy alta de servicios gratuitos de correo, especialmente Gmail. Según los datos más recientes disponibles[68], en Chile aproximadamente el 67.3 % de los residentes utilizan Gmail como su proveedor principal de correo personal libre, una de las cifras más altas a nivel regional. Estudios sobre marketing digital en LATAM indican que los proveedores más utilizados en campañas masivas siguen siendo Gmail, Outlook/Hotmail y Yahoo, cubriendo más del 70 % del ecosistema regional de correos personales[69].

En conjunto, estas cifras muestran que una proporción muy significativa de la población —tanto global como especialmente latinoamericana— utiliza Gmail como correo personal. Esto implica que la compatibilidad (o incompatibilidad) entre la Google Dot Rule y los procesos internos de registro, validación y depuración de correos electrónicos dentro de las organizaciones no es un riesgo marginal, sino uno con impacto poblacional, regulatorio y operacional. En consecuencia, cualquier desviación en la calidad del dato, procesos de normalización o revocación del consentimiento puede afectar directamente a millones de usuarios, elevando la criticidad de este riesgo dentro de los modelos de cumplimiento y gestión de privacidad.

V. Jurisprudencia y sanciones.

Dado que la protección de datos personales es un ámbito aún incipiente en Latinoamérica —con leyes recientes como la Ley 21.719 en Chile o la LOPDP en Ecuador— y con autoridades en fase temprana de implementación, resulta relevante analizar la experiencia de jurisdicciones más consolidadas, como España. En este sentido, la jurisprudencia de la Agencia Española de Protección de Datos (AEPD) ofrece un marco de referencia útil para comprender cómo los

[65] https://www.demandsage.com/gmail-statistics
[66] https://clean.email/blog/email-providers/most-popular-email-providers
[67] https://www.demandsage.com/gmail-statistics
[68] https://worldpopulationreview.com/country-rankings/gmail-users-by-country
[69] https://selzy.com/en/blog/latam-email-marketing

errores en la gestión del correo electrónico pueden constituir infracciones relevantes, aun cuando no existan sanciones específicas relacionadas con la Google Dot Rule.

Es importante precisar que no existe, hasta la fecha, evidencia pública de sanciones en Latinoamérica directamente asociadas al uso o desconocimiento de la Google Dot Rule, lo cual es esperable dada la reciente entrada en vigor o modernización de las leyes locales. Tampoco la AEPD ha emitido resoluciones que sancionen expresamente incidentes derivados de esta regla técnica de Gmail. Sin embargo, sí existen numerosos expedientes sancionatorios que abordan errores derivados del uso incorrecto del correo electrónico, todos ellos extrapolables a los riesgos que pueden materializarse cuando las organizaciones no gestionan adecuadamente la calidad, unicidad o validación de direcciones de correo electrónico. Algunos ejemplos relevantes son:

- Procedimiento PS-00566/2024, en el cual la AEPD sanciona a una entidad por enviar información personal a destinatarios incorrectos debido a errores en la gestión interna de datos de contacto. Este caso resulta especialmente pertinente, pues demuestra que una falla en los procesos de registro, verificación o actualización de correos electrónicos puede conducir a un incidente de comunicación indebida.
- Otras resoluciones de la AEPD también sancionan prácticas como:
    - El envío de comunicaciones a cuentas equivocadas debido a duplicidades o errores de digitación.
    - La existencia de bases de datos sin depuración, generando envíos indebidos.
    - El uso de datos desactualizados que terminan filtrando información a terceros no autorizados.

Estos casos ilustran una conclusión clave: las autoridades de protección de datos sancionan el tratamiento incorrecto de correos electrónicos cuando ello produce filtraciones, revelación accidental, uso indebido o tratamiento no autorizado de datos personales, aun cuando la causa raíz sea un error operativo, administrativo o tecnológico.

En esa lógica, si una empresa desconoce el funcionamiento de la Google Dot Rule y no implementa controles para evitar duplicidades o variantes equivalentes de un mismo correo, los riesgos derivados —como comunicaciones indebidas, vulneración del consentimiento o imprecisión del dato— serían imputables a la organización, no al proveedor del servicio de correo.

Por tanto, aunque la Google Dot Rule no genera por sí misma un incidente, la falta de adecuación de las empresas a una regla técnica conocida, documentada y pública, sí puede traducirse en infracciones sancionables por principios como:

- Exactitud del dato (AEPD, RGPD art. 5.1.d / Ley 21.719 art. 8.b)
- Limitación de la finalidad

- Seguridad del tratamiento
- Integridad y confidencialidad
- Responsabilidad proactiva (accountability)

En consecuencia, la jurisprudencia española refuerza que la adecuada gestión del correo electrónico es esencial, y que los errores en este ámbito —incluyendo aquellos que podrían derivarse del desconocimiento de la Google Dot Rule— pueden constituir infracciones significativas bajo marcos regulatorios de protección de datos.

VI. Riesgos de privacidad derivados del Dot Rule.

A pesar de que la Google Dot Rule es un comportamiento documentado y perfectamente conocido del servicio Gmail —no un defecto ni una vulnerabilidad— muchas organizaciones en Latinoamérica estructuran sus procesos, bases de datos y sistemas de comunicación sin contemplar este comportamiento técnico. Esta desconexión entre el diseño de Gmail y las prácticas corporativas genera escenarios donde variantes aparentemente distintas de una dirección (con puntos, sin puntos o con alias "+") son tratadas como identidades separadas, aun cuando corresponden a un mismo buzón. El resultado no es atribuible a Google, sino a **fallas en la gestión del dato**, **ausencia de controles de calidad**, y **desalineación entre procesos legales, TI y operaciones**.

La relevancia de estos riesgos aumenta en el contexto de las nuevas legislaciones latinoamericanas —como la Ley 21.719 de Chile, la LOPDP de Ecuador y marcos inspirados en el RGPD— que exigen estándares más estrictos de exactitud del dato, licitud del tratamiento, respeto al consentimiento y adopción de medidas razonables de seguridad. Cuando las organizaciones no normalizan las direcciones Gmail, los flujos de comunicación pueden derivar en envíos cruzados, tratamiento indebido, violaciones de consentimiento, o entrega no autorizada de información, lo que configura incidentes de protección de datos.

En este contexto, los principales riesgos derivados del desconocimiento o mala implementación del tratamiento de direcciones Gmail incluyen:

- **Fuga de información entre clientes que comparten variantes equivalentes.**

Cuando dos clientes registran variantes equivalentes bajo Dot Rule, la empresa puede creer que son personas distintas; sin embargo, Gmail entregará la información al mismo receptor.

- **Violación de consentimiento cuando no se normalizan direcciones.**

Si el titular revoca consentimiento sobre una variante, pero la empresa mantiene otra versión equivalente, continuará enviando comunicaciones no autorizadas.

- **Incumplimiento del principio de exactitud del dato, transparencia y minimización.**

El mantenimiento de múltiples variantes para un mismo usuario contraviene obligaciones de mantener la información exacta y actualizada.

- **Envío ilegal de comunicaciones tras revocación.**

Un error común es eliminar el correo "con punto" pero mantener el "sin punto",

provocando envíos ilegales desde el punto de vista normativo.

- **Incidente reportable ante la Ley 21.719.**

Si se envía información personal a una variante no autorizada que llega al titular equivocado, se configura un incidente que podría ser reportable ante la autoridad.

VII. Ejemplos prácticos

Para comprender la materialización del riesgo asociado al Google Dot Rule —derivado no de un error de Gmail, sino de la falta de normalización y control por parte de los responsables del tratamiento— resulta útil revisar escenarios concretos donde esta incompatibilidad técnica-operativa puede generar vulneraciones al principio de exactitud, entregas indebidas de información y tratamientos ilícitos. Los siguientes casos ilustran situaciones frecuentes en organizaciones latinoamericanas y evidencian cómo este riesgo se manifiesta en contextos reales.

Ejemplo 1 — Dos clientes, un mismo inbox

Un primer cliente registra *lucas.rojas@gmail.com* y un segundo cliente registra *lucasrojas@gmail.com* como correos distintos dentro del sistema. Para Gmail, ambas direcciones son equivalentes y se entregan al mismo titular. La empresa, desconociendo esta equivalencia, puede enviar información personal del segundo cliente al primero, generando una fuga de información.

Ejemplo 2 — Revocación de consentimiento

Un titular revoca el consentimiento para recibir comunicaciones en *lucas.rojas@gmail.com*, y la empresa elimina únicamente esa variante. Sin embargo, una versión equivalente (*lucasrojas@gmail.com*) permanece en sus sistemas y continúa recibiendo mensajes. Esto configura un envío no autorizado, vulnera la revocación del consentimiento y constituye un tratamiento ilícito derivado de una base mal gestionada.

VIII. Mitigaciones legales, técnicas y operacionales

La gestión del riesgo asociado al Google Dot Rule no depende de corregir una funcionalidad de Gmail —pues no es un error— sino de fortalecer las prácticas internas de las organizaciones. La mitigación requiere un enfoque integral que combine requisitos jurídicos, medidas técnicas y disciplina operativa en la administración de datos personales. Solo una aproximación holística permite asegurar que los tratamientos se ajusten a los principios de exactitud, licitud y minimización establecidos por las normativas de protección de datos.

a) Mitigaciones legales

Desde la perspectiva jurídica, la mitigación implica incorporar explícitamente la normalización de correos y la verificación reforzada como medidas de seguridad exigibles bajo el principio de exactitud y calidad del dato. También requiere protocolos claros para cambios de direcciones, revocación de consentimiento y trazabilidad de decisiones, a fin de garantizar un tratamiento lícito conforme a la Ley 21.719, la LOPDP y el RGPD.

b) Mitigaciones técnicas

En el ámbito técnico, la clave está en adoptar mecanismos que permitan identificar, unificar y bloquear variantes

equivalentes de cuentas Gmail antes de que ingresen a los sistemas. Esto incluye incorporar algoritmos de normalización, validaciones activas de correo y controles antifraude que aseguren que cada titular tenga un único registro operativo, reduciendo el riesgo de fugas y envíos indebidos.

c) Mitigaciones de procesos y gobierno

Operacionalmente, la mitigación requiere estándares de calidad del dato, procedimientos de revisión periódica de bases, y coordinación entre áreas legales, TI y negocio para asegurar consistencia en la captura, actualización y uso de direcciones electrónicas. La gobernanza adecuada del dato se transforma así en un elemento esencial para prevenir incidentes y sostener el cumplimiento continuo.

José Antonio Berrios Paredes

Chile

Director de Seguridad de la Información, QQRucho Legal & Tech

Consultor en Protección de Datos y Ciberseguridad

Contacto: jose.berrios@gmail.com

Sobre propiedad intelectual, licencias, derechos y contexto en Argentina y el software

Ash Pablovich

Índice

Definiciones

La propiedad intelectual se refiere a bienes económicos y culturales que pueden ser tanto intangibles como físicos. Según la Organización Mundial de Propiedad Intelectual (OMPI), incluye cualquier creación de la mente humana, pero jurídicamente, es lo protegido por las leyes de propiedad intelectual, y cualquier creación intelectual no reconocida por las leyes no se considera como tal. En general, las legislaciones formales no incluyen a todos los tipos de creaciones, sino algunas específicas bien definidas como obras literarias, marcas, diseños industriales, y no, por ejemplo, un número o un color (aunque depende del contexto [1]).

Respecto a su alcance, puede pertenecer tanto a un solo a autor como a varios en el

caso de creaciones en colaboración o grupales, y generalmente se les otorga derecho de propiedad hasta cierto plazo luego de su fallecimiento, pudiendo después ser heredado o pasado a dominio público.

Existen distintos tipos de derechos que protegen la propiedad intelectual. Puede ser confuso porque se suelen usar varios de estos conceptos como sinónimos, por eso vamos a explicarlo dividiéndolo en dos ramas, siendo la primera en la que más vamos a profundizar.

Derechos del autor

Protegen obras científicas, literarias y artísticas de cualquier tipo. Abarcan la expresión de ideas, conceptos y procedimientos, pero no a esas ideas en sí [2], esto significa, por ejemplo, que un pintor puede ser dueño de sus pinturas, pero no evitar que otros hagan pinturas con los mismos materiales sobre el mismo tema, o que un matemático es dueño del libro donde publicó sus ecuaciones, pero no puede evitar que otros científicos las usen en sus cálculos. Lo que sí protege es que las obras puntuales donde desarrollaron esas ideas no se puedan copiar, publicar o comercializar sin su permiso.

Propiedad industrial

Otorga derechos sobre las invenciones dentro de la industria y comercio, incluyendo marcas, patentes, diseños industriales, modelos de utilidad, nombres comerciales e indicaciones geográficas.

Las licencias, algo de lo que también se suele hablar en este ámbito, son acuerdos para los bienes protegidos por derechos del autor donde el autor permite a otras personas hacer uso de ellos mientras se cumplan ciertas condiciones. No quitan los derechos de autor sobre una obra sino que los complementan. Vamos a hablar de tres tipos [3].

Copyright

Es la licencia "clásica" que reserva todos los derechos de uso al autor (los que otorgue la ley en el país correspondiente), y expresa que no da ningún permiso a otros sobre ella.*Copyleft*

Su nombre hace referencia a ser el opuesto de *copyright*, y permite el libre uso y distribución de la obra, exigiendo que se preserven las mismas libertades sobre sus copias y derivados, para protegerla de la privatización. Surgió en el área del software libre y la más conocida es GNU General Public License.

Creative Commons

Creative Commons es una organización sin fines de lucro que se dedica a promover el acceso e intercambio de cultura. Desarrollaron un conjunto de licencias que ofrecen a quienes las usa una manera simple y estandarizada de compartir su trabajo al público bajo las condiciones de su elección. Sus licencias están compuestas por cuatro módulos de condiciones:

- *Attribution* / *Atribución* (BY): requiere la referencia al autor original.
- *Share Alike* / *Compartir Igual* (SA): permite obras derivadas bajo la misma licencia o similar.

- *Non-Commercial* / *No Comercial* (NC): prohibe que la obra sea utilizada con fines comerciales.
- *No Derivative Works* / *No Derivadas* (ND): no permite modificar la obra de ninguna manera.

En base a estos módulos existen seis licencias CC que son combinaciones de ellos (CC BY, CC BY-SA, CC BY-ND, CC BY-NC, CC BY-NC-SA y CC BY-NC-ND).

Otras licencias que existen además de las mencionadas son las licencias permisivas (permiten uso y modificación incluso para fines comerciales con pocas condiciones, ej: Apache), el dominio público (cuando el autor renuncia a sus derechos o expiró el plazo legal luego de su fallecimiento), y licencias académicas / de documentación (por ejemplo para bases de datos abiertas, como OpenStreetMap).

En resumen, podríamos decir que la propiedad intelectual son los bienes creados por la mente humana que están protegidos legalmente, entre los derechos que la protegen están los derechos del autor, y sobre las obras protegidas por derechos del autor se pueden aplicar licencias para que su autor otorgue los permisos que quiera.

Legislación en Argentina

La ley que reconoce el derecho del autor es la 11.723. Esta ley expresa qué tipo de obras protege, qué derechos otorga a su autor, cuáles son las penas, y otras cuestiones como casos específicos, cómo tratar la colaboración entre autores, obras extranjeras y cómo son los procedimientos de registro y denuncia.

"A los efectos de la presente Ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas, en fin, toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción.

La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí."

Ley 11.723. Régimen de propiedad intelectual. Art 1°.

El resto de bienes de propiedad intelectual, que entran en propiedad industrial, están protegidos por la ley 24.481 de patentes de invención y modelos de utilidad, que reconoce justamente esos dos títulos de propiedad, y la ley 22.362 de marcas y designaciones que especifica sobre marcas registradas.

En lo que respecta a tratados internacionales, Argentina firmó los siguientes [4]:

Tratado de la OMPI sobre interpretación o ejecución y fonogramas (TOIEF) (2002)

Tratado de la OMPI sobre derechos de autor (TODA) (2002)

Acuerdo sobre los aspectos de la propiedad intelectual ligados al comercio (ADPIC) (1995)

Convenio para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas (1973)

Convención internacional sobre la protección de artistas intérpretes o ejecutantes, productores de fonogramas y organismos de radiodifusión (1992)

Convención universal sobre derechos de autor (1952)

Convenio estableciendo la Organización Mundial de la Propiedad Intelectual (1980)

Convenio de Berna para la protección de las obras literarias y artísticas (2000)

Convención interamericana sobre derecho de autor de las abras literarias, científicas y artísticas (1953)

Convención internacional americana sobre propiedad literaria y artística (1949)

Tratado de Montevideo sobre propiedad literaria y artística (1894)

Si hablamos de derechos de autor, podemos decir que el más conocido/relevante es el Convenio de Berna, siendo la base de los derechos de autor en el mundo, que establece principalmente que las obras están protegidas desde el momento de su creación, los autores extranjeros reciben la misma protección que los locales, y fija un plazo de protección post mortem de 50 años (Argentina lo amplía a 70). También es importante el TODA, que amplía y regula el derecho en el área digital y de Internet.

Que las obras estén protegidas desde su creación significa que no es obligatorio registrarlas para recibir protección, pero es recomendable para servir como evidencia en caso de plagio. El registro se hace en la Dirección Nacional de Derechos del Autor.

En lo que respecta a licencias, cuando se quiere otorgar permisos a una persona específica, la licencia se puede ver como un contrato entre dos partes, el autor y un tercero, y este se contrato se debe registrar también en la DNDA. Es por ejemplo el caso de un autor que quiere publicar su libro en una editorial y les da permiso de copia y comercialización. Pero en el caso de las licencias libres, que son hacia el público, no hay contrato porque no hay una segunda parte y basta con que quede declarado públicamente (como el típico archivo LICENSE al descargar un software).

¿Dónde entra el software?

Ahora que vimos qué es la propiedad intelectual, los tipos de derechos y licencias que hay, y cómo están reglamentados en nuestro país surge la pregunta de cómo se aplica en nuestra área.

El software es esencialmente distinto a otros productos y obras y suele ser difícil de clasificar. ¿Es más parecido a un libro o a una máquina industrial? Es intangible, abstracto y su proceso de producción es intelectual, como una obra literaria, pero

sigue (idealmente) los pasos rigurosos de una ingeniería y se documenta en diagramas que se asemejan a planos de construcción. Surge de un proceso creativo, pero se consume como una herramienta de trabajo. ¿Por qué derechos corresponde, entonces, que sea protegido? La respuesta que dan la mayoría de legislaciones, incluyendo la de Argentina, es incluirlo en los derechos de autor junto a las obras científicas y artísticas.

No solo los programas de computación son mencionados en la ley 11723, sino que son explícitamente excluidos de ser patentados como tales en la ley 24481.

"No se considerarán invenciones para los efectos de esta ley:

[...]

c) Los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, así como los programas de computación;

[…]"

Ley 24481. Patentes de invención y modelos de utilidad. Art 6°.

Cabe aclarar que es distinto el caso de un producto físico que incluya hardware y software, en el cual sí podría ser patentado, pudiendo a su vez el software que usa ser protegido por derechos del autor por separado, como por ejemplo una marca de celulares y su sistema operativo.

En la siguiente sección vamos a mostrar brevemente ejemplos [5] de cuestiones y dilemas que han surgido respecto al software y los derechos de autor y cómo se resolvieron.

Casos ejemplares y discusión

Caso Apple vs Franklin: formatos de código

Apple había lanzado en el año 1977 sus computadoras *Apple II*. En 1982 la empresa Franklin Computer Corporation introdujo en el mercado el modelo *Franklin Ace 100* que era un clon de las computadoras de Apple. Se determinó que gran parte de su código había sido copiado del firmware de *Apple II* (Incluso aparecía el nombre de la empresa y sus programadores). Se inició una demanda por infracción a los derechos del autor.

La empresa demandada argumentó que solamente había copiado una parte, la memoria ROM, y era necesario hacer una réplica para mantener compatibilidad con los programas de Apple, pero mostraron que se podría haber escrito de manera diferente y habían otros ejemplos compatibles en el mercado que no se copiaron. También se defendieron diciendo que solo el código fuente (legible para humanos) podía ser protegido por copyright, y no el código objeto (compilado/ejecutable), pero la corte rechazó este argumento y declaró que el copyright extiende a cualquier forma tangible de expresión mediante la cual se pueda comunicar no solo directamente, sino también con ayuda de una máquina.

Computer Associates International vs Altai, Inc: copias literales y no literales

El contexto de este caso es un programa desarrollado por CA para las computadoras de IBM, llamado CA-SCHEDULER, que

servía para planificar tareas, y contenía un subprograma llamado ADAPTER, el cual era una parte esencial del mismo.

La empresa ALTAI también tenía un programa para planificación de tareas, OSCAR, y el empleado (luego jefe) James Williams contrató al desarrollador Claude Arney que había sido empleado de CA y conocía muy bien el módulo ADAPTER, para desarrollar una nueva versión de OSCAR adaptarda a otro sistema operativo. El resultado fue que Arney copió el 30% del código de ADAPTER en OSCAR 3.4, lo que causó que fueran demandados por plagio.

Como había sido una copia literal del código fuente, reconocieron haberlo hecho y no apelaron a la condena. Lo interesante es lo que pasó después, cuando Williams tomó el consejo de su abogado y reescribió todo el código que había sido copiado. Arney fue excluído del proceso y su copia de ADAPTER fue destruída, y comenzaron a vender la versión OSCAR 3.5. Aún así, CA denunciaba que seguía habiendo plagio porque la estructura del programa, es decir, la comunicación entre funciones y sus parámetros y el diagrama de flujo general eran “sustancialmente similares”. Como ya no era literalmente el código de su programa, sino que a grandes rasgos tenía una forma parecida, entramos en un caso del debate entre idea y expresión.

Para tomar una decisión, se decidió analizarlo en tres partes: la abstracción (¿En qué nivel de abstracción del software deja de ser expresión y pasa a ser idea, siendo el más bajo el código fuente y el más alto la idea básica de su funcionalidad?), el filtrado de elementos (¿Cuáles son similares por copia y cuales lo son por casualidad o tomados del conocimiento público? es difícil construir un software para un propósito sin seguir ciertas prácticas o formas estándar), y por último, luego de haber decidido el nivel de abstracción a tomar en cuenta y filtrado los elementos que se consideraban incidentales o comunes, hacer una comparación. Se decidió que no existía una similitud sustancial, y la corte falló en contra del demandante para OSCAR 3.5.

Mi opinión como estudiante del área del software

Considero que en los ambos casos la decisión de la corte fue acertada, aunque en el segundo da lugar a más discusión. Me parece importante aclarar algunos aspectos del área para entenderlo.

En el primer caso, el código objeto es el resultado de traducir el código fuente, escrito en un lenguaje de programación, a código para máquina que la computadora puede ejecutar. No protegerlo sería tan absurdo como permitir plagio de cualquier obra mientras se encripte con una operación matemática y se necesite un programa para desencriptarlo. Es más, cualquiera podría escribir un programa que muestre en pantalla un libro o video musical, compilarlo y eliminar el código fuente, y estar exento de acusaciones de plagio.

En el segundo caso, es más complejo porque hay grises en la definición de en qué nivel de abstracción se pasa de lo concreto a la forma. Personalmente considero que lo que está a nivel más alto que el código fuente (diagramas de clase o

flujo, por ejemplo, que expresan la forma y comportamiento de los datos), se puede considerar como idea y no expresión, descartando así las acusaciones. Cuando se analiza el origen de la similitud, hay algo de razón en pensar que no fue incidental sino el resultado del refactoring de una copia, pero en el diseño de software hay prácticas, patrones y modelos de arquitectura que definen soluciones a nivel tan concreto y para tantos casos específicos, que es no solo fácil sino esperable terminar con modelos similares. Consideremos también que el estilo de escritura de código y diseño de soluciones se va formando en base a quienes tomamos de referencia o con quienes trabajamos, que dejan huellas inconscientes en nuestra forma de pensar así como pasa con artistas y escritores. Teniendo en cuenta todo esto, yo no tomaría similitudes de alto nivel de abstracción en el software como acusables de plagio, aunque no descarto la posibilidad de excepciones.

Crítica filosófica y política

Para finalizar me parece buena idea mencionar críticas que han surgido respecto al concepto de propiedad intelectual.

Hay quienes consideran que los derechos de autor no benefician a la sociedad porque restringen el acceso a la información y la cultura y desincentivan la creación de mayor conocimiento.

Por otro lado, también se critica el lado económico, argumentando que la propiedad intelectual es inválida porque, a diferencia de la propiedad física, no hay escasez, y su infracción no priva al autor de su obra como el robo. Una frase popular que ha surgido, especialmente en el contexto de la creciente economía de suscripciones, es *"If buying isn't ownership, piracy isn't theft"* ("Si comprarlo no es ser dueño, piratearlo no es robarlo").

Algunos grupos de personas que se oponen a esto abogan por la abolición de la propiedad intelectual o incentivan su infracción, mientras que otros proponen el uso de alternativas más libres dentro del marco legal actual, surgiendo de ahí el copyleft y Creative Commons.

Es cierto que durante toda la historia las personas han producido obras científicas, artísticas y tecnológicas sin incentivo económico, y movimientos como el software libre han demostrado lo que se puede lograr con trabajo abierto y colaborativo. Tiene sentido, sin embargo, que dentro del sistema económico, cuando el crecimiento deja de pasar por la producción de manufacturas físicas en sí y se centra en los avances científicos, tecnológicos y de entretenimiento, surjan formas de tratar las invenciones como propiedad, para que las corporaciones puedan crecer en base al monopolio y los creadores pequeños puedan aferrarse a la exclusividad de su obra como algo que les de sustento económico. Puede que sea a cambio de injusticia en algunos aspectos y peor desarrollo cultural, pero en todo caso no sería algo específico de la propiedad intelectual sino extrapolable a cualquier otra forma de propiedad privada.

Notas

[1] Existen casos donde empresas han registrado con copyright el color de su marca, lo cual está permitido siempre y cuando sea un tono bien definido, sea percibido por el público como identificador de esa marca, y no sea un color básico o ampliamente usado en la industria (ej: rojo en una marca de matafuegos). Solo se otorga derecho al uso exclusivo de ese color dentro de ciertos productos o servicios de ese sector.

[2] La distinción entre idea y expresión no siempre es fácil de definir y se suele debatir en cada caso.

[3] Me refiero a "tipos" de licencias porque se pueden categorizar por el grado de libertad que otorgan u otras características, pero dentro de cada uno hay varias específicas.

[4]Los años corresponden a desde cuándo tienen vigor en el país, no cuándo fueron escritos.

[5] Los ejemplos que encontré para mostrar son extranjeros, por lo que no procederían exactamente igual con nuestro modelo judicial y leyes, pero los principios que se plantean nos interesan.

Bibliografía y fuentes

Wikipedia

Legislación y casos de propiedad intelectual - Carlos A. Palazzi

leyes-ar.com - buenosaires.gob.ar

DNDA

pablomazaabogado.es

Estudiante de Licenciatura en Sistemas en la UNPSJB en Trelew, Chubut, Argentina - trabaja en desarrollo de software

SOMOS LA RED

- HOLA?
- EDI?

ELDERECHOINFORMATICO.COM

Neurointerferencias y vacíos legales: ¿estamos protegidos por la ley cuando la tecnología llega al cerebro?

Maria Eugenia Lo Giudice

I.- Introducción

Desde el momento en que la **mente humana**, hasta ahora considerada un reducto inviolable, se convierte en el nuevo objeto de observación, se desintegran conceptos tradicionales en cuanto protección de los datos que definen a la persona humana.

Desde el momento que la Sociedad del Conocimiento que transitamos actualmente, se centra en la propia actividad cerebral, nos obliga a replantear las categorías jurídicas clásicas.

II.- Nuevas categorías de Derecho ante la neurociencia

Luhmann[70] nos recuerda que el derecho reduce complejidad social creando conceptos que orientan la conducta, siguiendo este pensamiento frente a la complejidad que genera la neuro revolución que estamos atravesando, las neuro tecnologías demandan nuevas categorías jurídicas, que desde ya dejo planteadas siguiendo a las propuestas por el Dr. Roberto Andorno y Marcello Lenca en el año 2017, ellas serían: libertad cognitiva , privacidad mental, identidad neuropsicológica, reconociendo asimismo

[70] Luhmann, Niklas. Sociólogo alemán, 1927-1998, conocido por su Teoria General de los Sistemas Sociales

las que se venían tratando respecto a la protección contra los sesgos algoritmitos y respetando el acceso equitativo, en este caso acceso equitativo neuronal.

Pero antes de entrar un poco más en detalle respecto de las nuevas categorías mencionadas, quisiera destacar la importancia de la protección de estos nuevos tipos de "datos", hasta el punto de poder influir en la suma de las voluntades que conforman la sociedad misma. Porque si la legitimidad democrática depende de la autonomía de la voluntad, y ésta autonomía se puede ver condicionada por las tecnologías que pueden alterar decisiones, entonces la democracia misma se encuentra en riesgo.

Incluso se puede generar un debilitamiento de los vínculos sociales si se favorecen estructuras de poder que priorizan la eficiencia técnica, en este caso el binomio tecnología-neurociencia, sobre los "valores humanos", tal como lo viera Zygmunt Bauman[71].

Considero que no hay buenas o malas tecnologías por sí mismas, la tecnología es neutra. Es el propio ser humano quien debe decidir sobre su uso y aplicación. Si lo que se plantea es el riesgo de intervenir la mente humana, pues se debe proteger la "inviolabilidad" de la misma.

Urge que se respete un marco ético jurídico de la neuro tecnología, donde sea así considerado el resguardo a los neuro derechos como nueva categoría para evitar un futuro distópico, justamente el acceso irrestricto a la mente humana.

Con este objetivo desde el 2018 trabaja la UNESCO junto a expertos en la materia, y luego que en el 2021 se realizará una amplia consulta a nivel internacional, se ha logrado aprobar en noviembre del 2025, las recomendaciones sobre la ética de las neuro tecnologías. En palabras de su directora general, Audrey Azoulay: "La neuro tecnología tiene el potencial de definir la próxima frontera del progreso humano, pero no está exenta de riesgos. Con la adopción de este nuevo instrumento normativo, la UNESCO establece límites claros y consagra la inviolabilidad de la mente humana. Este texto encarna una profunda convicción: que el progreso tecnológico solo vale la pena si está guiado por la ética, la dignidad y la responsabilidad hacia las generaciones futuras."[72]

III.- Neurotecnología y privacidad personal

El campo de la neuro tecnología abarca ampliamente cualquier dispositivo o método electrónico que pueda usarse para leer o modificar la actividad de las neuronas en el sistema nervioso, es decir

[71] Zygmunt Bauman (2000), sociólogo polaco-británico conocido por su concepto de **"modernidad líquida"**, que describe una modernidad en la que nada parece perdurar y todo está en constante transformación, que puede provocarse profundas consecuencias para las personas y las sociedades

[72] Comunicado de Prensa, UNESCO, Noviembre 2025 https://www.unesco.org/es/articles/etica-de-la-neurotecnologia-la-unesco-adopta-la-primera-norma-mundial-para-esta-tecnologia-de

para describir, borrar e incluso “reescribir” sobre ese proceso.

Si las nnuevas tecnologías actualmente posibilitan acceder al cerebro humano, pudiendo obtener resultados científicos, clínicos, económicos, sociales, etc.., debe considerarse la invasividad que estas nuevas tecnologías pueden provocar en cuerpo y mente humana, debate de interés global e interdisciplinario, tanto de la neurociencia como de la bioética, biotecnología, sociología, etc.

Tanto los poderes públicos como los organismos regionales e internacionales competentes deben abordar la problemática, enmarcada en principios éticos y jurídicos para seguir preservando la dignidad de la persona, el respeto a los Derechos Humanos.

Hasta no hace mucho se reposaba sobre la tranquilidad que confería el Derecho, con el consenso nacional, internacional, privado o público, sobre la protección y respeto a la privacidad de las personas basado en el honor y la dignidad de la misma, cuestión que tuvo un largo desarrollo a través de los tiempos, desde su incipiente “derecho a no ser molestado” en 1890, a la no injerencia en los asuntos privados de las personas o derecho a la Privacidad, hasta la preservación de la esfera de los “datos personales” por ser quienes definen a los titulares de los mismos. Así quedaba al resguardo el ser humano como tal.

IV.- Información procedente del cerebro humano: dato neuronal

Se trata de preservar la “integridad mental”, disponiendo del libre albedrío que las convierten en un ser único, y protegiéndolas contra la discriminación o cualquier tipo de sesgo basados en algoritmos y ante el posible abuso de las tecnologías.

La legislación en general venía estudiando, reconociendo y protegiendo lo que hace al “tratamiento” de los datos personales. Se refiere al procesamiento que se hace de ellos, desde su recolección hasta su almacenamiento, pero actualmente vino a sumarse la “proyección” que se puede hacer de los datos personales.

Algunos autores consideran que: “existe la posibilidad, aunque no la probabilidad, de que los datos cerebrales recopilados que en sí mismos no parezcan identificar a un sujeto puedan, al reutilizarse o en combinación con otros datos, identificar a un sujeto de datos y fundamentar predicciones sobre dimensiones sensibles de su identidad.”[73]

Por lo que también a partir de la generación de este nuevo tipo de datos basados en la actividad neuronal, los datos neuronales, también podría llegar a identificar su emisor.

Por esto se necesita reconsiderar el concepto de “datos personales, y entran en acción los “datos neuronales”, producto de la actividad neuronal de las personas, que surgieron estudiados y tratados para beneficiar con extraordinarios logros a

[73] .Rainey, S.; Mc Gillivray, K. et al. (2020)

millones de personas en el ámbito de la salud, pero su utilización esta excediendo al mismo para pasar ampliamente a otros (podría impactar en la industria bélica, en la actividad comercial, etc. etc.).

Arribo a la idea de esta manera que se debe ampliar el sentido de privacidad como era entendido hasta no hace poco.

Por otra parte, si se observa un procesamiento de información y funciones cognitivas realizado mediante redes neuronales, lo que da de llamarse computación neuronal, surgen preguntas de advertencia, como, ¿qué ocurriría ante una interferencia en ese procesamiento de interfase "cerebro-computadora-cerebro"? ¿Se podría hackear la información para ser retransmitida a dispositivos neuro tecnológicos, con el consiguiente peligro físico, mental y psíquico?.

Impactan en estos procesos neuro tecnológicos cerebrales, diferentes técnicas que van desde la manipulación opto genética, a técnicas de estimulaciones transcraneales o modificaciones profundas, etc. que pueden generar múltiples resultados como amnesias locales, falsas memorias, etc. con el fin de corregir desordenes neurológicos (en padecimientos tales como el alzhéimer, epilepsia, ELA) aunque podrían provocar modificaciones en la personalidad a un punto que la persona no se reconozca como ella misma, dándose una disrupción en su autopercepción.

V.- Nuevos conceptos

Como mencioné ut-supra, en el año 2017 los doctores Roberto Andorno[74] y Marcello Lenca[75], publicaron su informe "Hacia nuevos derechos humanos en la era de la neurociencia y la neuro tecnología"[76], donde luego de analizar la relación entre neurociencia y derechos humanos proponen cuatro nuevos derechos.

1) Derecho a la Libertad Cognitiva: asimilable a la clásica "libertad de pensamiento". Se ejerce en función del libre albedrío de las personas, basado en la "autodeterminación mental". Tiene que ver con la intimidad mental.

Se puede ejercer a través de la modalidad de acción u omisión respecto a la neuro tecnología, ya sea como un derecho de acceso o como protección contra el uso coercitivo de la misma.

2) Derecho a la Privacidad Mental: protección necesaria a la actividad neuronal que genera información, en este caso los datos neuronales. Ámbito privado reservado para lo que piensa y lo que siente definiéndolo en su individualidad.

Se debe proteger la emisión de los datos neuronales producidos por las ondas cerebrales captadas tanto con conciencia de ello como sin conciencia, es decir sin conocimiento de su emisor. Justifica el

[74] Perteneciente al Swiss Federal Institute of Technology Zurich (ETH), Dept. of Health Sciences and Technology, Zurich, Suiza.

[75] Integrante de la Universidad de Zurich, Suiza

[76] Andorno, Roberto - Ienca, Marcello; "Towards New Human Rights in the age of Neuroscience and Neurotechnology", Rev. Life Sciences, Society and Policy, 2017.

rechazo a la manipulación externa de la mente.

3) Derecho a la Integridad Mental: protección de la estructura y funcionamiento del cerebro y su actividad frente a manipulaciones no autorizadas o intervenciones neuro tecnológicas que puedan alterar sin consentimiento, los procesos mentales de una persona. Derecho de todos los individuos a proteger su dimensión mental en el sentido amplio y actual ante posibles daños.

Puede hablarse de "brainhacking malicioso" para referirse a la posibilidad de influir o transgredir directamente en las redes neuronales de usuarios de neuro dispositivos tal como se hackean las computadoras.

La tecnología posibilita la interfase cerebro-computadora-cerebro, y ya se ha logrado comprobados efectos positivos, pero hay que prevenir la regulación frente a las posibilidades de las reacciones adversas.

4) Derecho a la Continuidad Psicológica: es la instancia especial del derecho a la identidad, en este caso a la identidad neuro-centrada.

Los cambios en la función cerebral causados por la neuro tecnología, como la estimulación cerebral, pueden generar alteraciones en los estados mentales críticos para la personalidad y por lo tanto pueden afectar a la identidad personal. Pueden provocarse cambios como que generen mayor agresividad, impulsividad o intolerancia en la persona.

Se trata del respeto a seguir siendo quien se siente quien es, a continuar una identidad psicológica, aunque no ocurriese un daño neurológico.

VI.- Opiniones encontradas

La incorporación de categorías como la libertad cognitiva, privacidad mental, identidad neuropsicológica y equidad neuro tecnológica conforman conceptos que no son meros neologismos académicos, sino construcciones sociales orientadas a preservar la dignidad humana en una era en la que lo más íntimo, como es la actividad mental, puede convertirse en objeto de regulación, vigilancia y explotación.

Según la UNESCO, 2023, la idea de los "neuro derechos" ha generado un animado debate entre los expertos, con preocupaciones que van desde que la creación de nuevos derechos podría socavar los derechos humanos existentes, hasta los retos prácticos de cómo definir y aplicar estos derechos.

Algunos han argumentado que el concepto de "neuro derechos" podría provocar una "inflación de derechos" o reducir la importancia de los derechos humanos existentes.

Otros han señalado que la noción de neuro derechos, sigue siendo ambigua y requiere mayor investigación para establecer definiciones claras y soluciones prácticas de algo novedoso pero carente de contenido.

La propuesta de neuro derechos se encuentra aún en una fase conceptual, pero hay coincidencia en la necesidad

urgente de que las legislaciones nacionales puedan contar con un marco ético global que oriente sus políticas y normativas para salvaguardar los derechos y libertades de los ciudadanos, las personas y las comunidades frente a los riesgos asociados a la neuro tecnología.

VII.- Conclusión

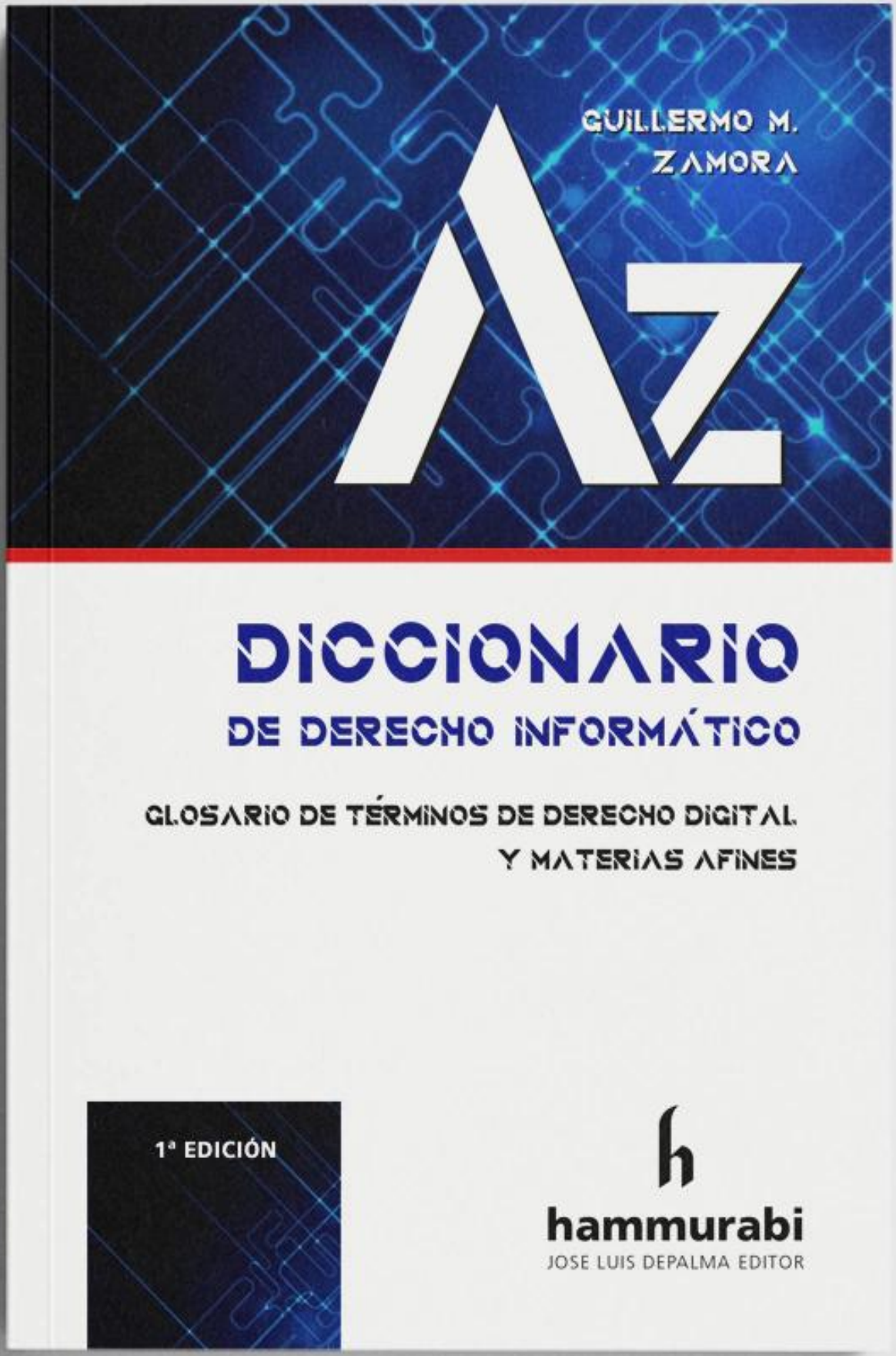
En definitiva, los neuro derechos constituyen un intento de garantizar que la autonomía, la dignidad y la igualdad permanezcan vigentes en un contexto donde las fronteras entre lo humano y lo tecnológico se desdibujan, donde el riesgo de colonización de la mente se convierte en una de las principales amenazas a la libertad contemporánea, pudiendo provocar serias brechas y conflictos sociales.

Por lo que cualquier diseño institucional o político debe tener como núcleo la preservación de la persona como fin en sí misma, incluso bajo condiciones distópicas donde la libertad se vea erosionada.

Haciendo un paralelismo respecto a lo que ya advierte Harari[77], el mayor riesgo no está en que la tecnología nos supere, sino en que aprenda a conocer nuestra mente mejor que nosotros mismos. De ahí la urgencia de construir un marco jurídico capaz de proteger lo único verdaderamente irremplazable: nuestra vida mental.

- Abogada (UBA, Argentina).
- Especialista en Derecho y Alta Tecnología.
- Doctoranda (Neuroderechos).
- Docente, Investigadora y Consultora.
- Con exposiciones y escritos en diversas Universidades nacionales/extranjeras
- Colaboraciones como Consultora en Agencias de Naciones Unidas y ONGs.

[77] Yuval Noah Harari es un historiador, filósofo y profesor israelí reconocido internacionalmente por sus análisis sobre la historia humana y el impacto de las tecnologías en la sociedad. autor de bestsellers como Sapiens, Homo Deus y 21 lecciones para el siglo XXI.



https://www.hammurabi.com.ar/productos/zamora-diccionario-de-derecho-informatico/

SOMOS LA RED

VAMOS DEJANDO HUELLA

ELDERECHOINFORMATICO.COM

IA hasta donde llegara la privacidad

Franco Maximiliano

Introducción

En este estudio nos adentramos en cómo la inteligencia artificial, en un futuro no muy lejano, podría transformar el mundo del derecho y lo legal.

Hay que fijarse, de la misma forma que el detector de mentiras en su día, las avanzadas tecnologías para el análisis cerebral, y en particular, las que se basan en modelos de aprendizaje automático aplicados a las imágenes por resonancia magnética funcional (fMRI), nos brinda una nueva ventana para explorar los patrones de nuestra mente, lo que permite interpretar ciertos aspectos del pensamiento humano.

Hace ya tiempo que la ciencia se ha propuesto entender qué pasa realmente en nuestra cabeza, ya ves. Y ser capaz de decodificar la actividad cerebral de un individuo, puede eso podría suponer avances en campo como la medicina, la psicología, incluso en la investigación científica. Pero con peligro, porque también nos obliga a plantearnos cuestiones muy serias sobre la privacidad de nuestra mente y sobre todo los límites éticos del saber. Lo que antes era cosa de ciencia ficción, ahora empieza a

materializarse como una posibilidad, que tiene la capacidad de cambiar nuestra forma de entender la verdad, la responsabilidad y la prueba dentro de los procesos legales.

Desarrollo

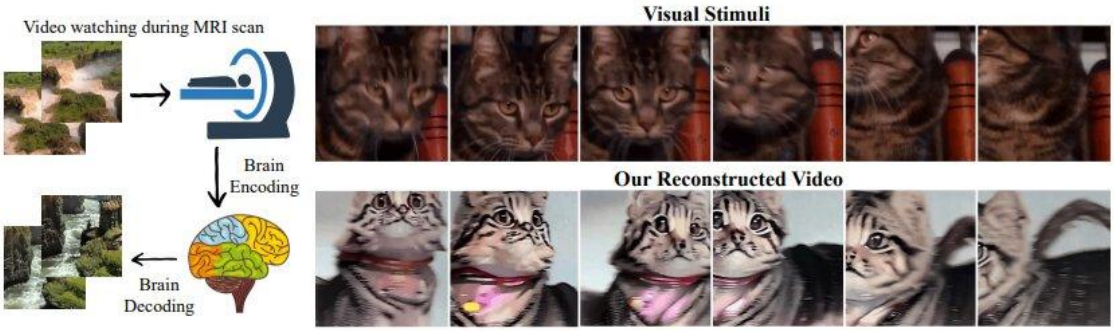
Aspectos técnicos.

Desde sus inicios, la base de este tipo de investigaciones se apoya en conocimientos y tecnologías médicas consolidadas, especialmente en el uso de la resonancia magnética funcional (fMRI) caracterizada por su alta resolución espacial y de los registros electroencefalográficos o magneto encefalográficos (EEG/MEG), que ofrecen una alta resolución temporal. Estas herramientas, que en su momento representaron un enorme avance tecnológico, permitieron observar y analizar la actividad interna del cuerpo humano, mejorando la detección de enfermedades y aumentando las expectativas de salud de la població

n.

Con la incorporación de la inteligencia artificial, estas técnicas alcanzaron un nuevo nivel. Al entrenarse modelos de *machine learning* con grandes conjuntos de imágenes médicas, se logró detectar ciertos tipos de cáncer con una precisión superior a la de médicos experimentados. La IA, al potenciar la interpretación de los datos biomédicos, se convirtió en una aliada esencial para el diagnóstico temprano y la mejora de la calidad de vida.

De la misma manera, los avances en prótesis inteligentes capaces de responder a estímulos neuronales o musculares representan una extensión natural de esta convergencia entre medicina e inteligencia artificial. Así como en su momento la resonancia magnética transformó la medicina, hoy la IA promete amplificar ese impacto, ofreciendo soluciones más



personalizadas y efectivas para mejorar la vida humana.

¿Podemos descifrar lo que sucede en nuestra mente?

En estos avances impulsados por la inteligencia artificial surgen los denominados decodificadores neuronales, sistemas que traducen la actividad cerebral en representaciones visuales comprensibles. Estos modelos utilizan redes neuronales y modelos generativos (como los basados en difusión) capaces de completar y recrear detalles visuales guiados por las señales cerebrales.

El procedimiento se basa en mapear la actividad cerebral de cada individuo mediante resonancia magnética funcional (fMRI). Durante el experimento, a los participantes se les muestran diferentes imágenes o videos mientras se registra la respuesta de distintas regiones del cerebro, especialmente en la corteza visual. Cada estímulo visual activa un patrón neuronal específico. Esos patrones se almacenan y forman un dataset personalizado que vincula "qué se vio" con "qué patrón cerebral se generó".

Posteriormente, los investigadores presentan nuevas imágenes o permiten que el participante imagine o sueñe con los mismos estímulos. Al comparar la nueva actividad cerebral con el mapa previamente aprendido, la IA es capaz de decodificar y reconstruir una aproximación visual de lo que la persona vio o imaginó.

La imagen anterior ilustra este proceso: en la parte superior se observa el estímulo visual original (un gato), y debajo, la reconstrucción generada por IA a partir de la actividad cerebral registrada. Aunque las reconstrucciones no son idénticas, muestran una notable coherencia con los patrones visuales del estímulo real, lo que demuestra el potencial de esta tecnología para vincular datos neuronales con representaciones mentales.

Desafios que superar.

Las limitaciones técnicas actuales de estos procedimientos son significativas. El uso de fMRI requiere equipos clínicos altamente costosos, y los datos obtenidos suelen ser ruidosos y complejos de interpretar. Además, los modelos deben ser entrenados de forma individualizada, ya que las funciones cerebrales y los patrones de activación varían entre personas. Esto implica que, por el momento, no es posible construir un *dataset* generalizado capaz de decodificar con precisión la actividad cerebral de cualquier individuo.

Otra restricción importante radica en la dependencia del sujeto de estudio, cuya colaboración activa es esencial para obtener resultados coherentes. La falta de estandarización dificulta la transferencia de modelos entre distintos participantes o contextos.

También se deben considerar los sesgos inherentes a los modelos generativos, los cuales pueden introducir interpretaciones erróneas o reconstrucciones inventadas. Dado que se trata de información vinculada directamente con la mente humana, estas distorsiones podrían tener consecuencias éticas profundas, como la atribución incorrecta de pensamientos o recuerdos. La cautela, por tanto, es indispensable: aunque los avances son

prometedores, aún estamos lejos de una decodificación cerebral universal y confiable.

Ética y derechos cognitivos

Chile se convirtió en el primer país del mundo en legislar sobre las neuro tecnologías, incorporando los denominados neuro derechos a nivel constitucional. Este hecho histórico ocurrió en octubre de 2021, cuando el Congreso aprobó una reforma que establece que el desarrollo científico y tecnológico debe estar al servicio de las personas, garantizando el respeto a su integridad física y mental.

La modificación constitucional incorporó explícitamente la protección de la actividad cerebral y de toda la información derivada de ella. En este marco, los neuro datos entendidos como los registros o mediciones de la actividad cerebral se reconocen con un estatus equivalente al de un órgano humano, lo que implica que no pueden ser comprados, vendidos, traficados ni manipulados. Esta protección busca anticipar un futuro en el que las tecnologías capaces de leer, alterar o reproducir procesos mentales sean una realidad cotidiana.

A diferencia de Chile, Argentina y otros países latinoamericanos aún no cuentan con marcos legales específicos que regulen este tipo de información. Existen casos preocupantes en los que personas han cedido, por desconocimiento o necesidad económica, datos biométricos altamente sensibles como escaneos del iris o información facial sin comprender las posibles consecuencias de su uso indebido.

El enfoque chileno representa una visión anticipatoria, ya que diversos expertos prevén que los avances de la inteligencia artificial aplicada a la neurociencia podrían permitir, en un futuro no muy lejano, leer directamente pensamientos, implantar emociones artificiales o comprometer la privacidad mental. En este contexto, los neuro derechos emergen como una defensa esencial frente a los riesgos éticos y sociales de una tecnología que, al adentrarse en la mente humana, toca el núcleo mismo de la libertad individual.

Un retroceso en el sistema judicial ¿volvemos a la cacería de brujas?

La perspectiva de usar tecnologías para descifrar la actividad cerebral en el mundo judicial genera un intenso debate sobre los límites del derecho, junto al respeto por las garantías individuales protegidas en la Constitución Nacional Argentina, si?

Pues los artículos 16, 18 y 19, cabe destacar que ellos definen los fundamentos clave del sistema legal, como la igualdad ante la ley, el proceso justo, y la inviolabilidad de la intimidad y la libertad de pensamiento.

El artículo 16 dice que “la Nación Argentina no acepta privilegios basados en linaje o nacimiento; no existen fueros personales ni títulos nobiliarios” y, que “todos sus ciudadanos son iguales ante la ley”, ¿verdad? Implementado en el dominio de la inteligencia artificial y las neuro tecnologías, este principio implica, que nadie debería ser juzgado o discriminado

según patrones neuronales, predisposiciones biológicas o interpretaciones algorítmicas de su mente, ¿que piensas? Aceptarlo introduciría una nueva forma de desigualdad, ¡la de los “cerebros transparentes” en comparación con aquellos que aún pueden resguardar su privacidad mental!

El Artículo 18, para empezar, blinda contra cualquier tipo de coacción o evidencia recogida de maneras que mancillen la dignidad humana: "Nadie se le puede obligar a declarar en su contra". Una tecnología capaz de revelar pensamientos o emociones sin un consentimiento total, ese principio de no autoincriminación lo dejaría en aprietos. La decodificación cerebral sin permiso o bajo presión judicial sería un nuevo tipo de tortura, no tan evidente, pero aun así violaría los derechos humanos elementales.

Por último, el Artículo 19 define un espacio sagrado: “Los actos privados de los hombres que de ninguna forma hieran el orden ni la moral pública, ni perjudiquen a terceros, solo están reservados a Dios y fuera de la competencia de los magistrados”. Este artículo protege la esfera personal de ideas, deseos y pensamientos, justo el dominio que las neuro tecnologías pretenden conquistar. Si el Estado o un tribunal tuvieran acceso a la mente de alguien para decidir su “posible culpabilidad”, volveríamos simbólicamente a los tiempos de la inquisición, donde se juzgaba más las intenciones que los hechos.

En este contexto, emplear la inteligencia artificial sin discernimiento, pretendiendo "leer la verdad" en los juicios, podría significar un paso atrás para nuestra civilización, un resurgimiento de la desconfianza y el castigo anticipado. Aún con toda la precisión que posean esas herramientas tecnológicas, jamás deberán sustituir los valores éticos y legales que cimientan el Estado de Derecho. La verdad descubierta por la ciencia no debe tener la potestad de someter la dignidad humana, ni tampoco la libertad interna de nuestros pensamientos.

Es por esto que el reto real no solo reside en qué tan lejos pueda avanzar la ciencia, sino en cuán fuertes se mantienen las barreras éticas y constitucionales que salvaguardan lo más preciado del ser humano: la autonomía de su mente.

La frontera entre mente y verdad?

En el fondo, lo que realmente está en hilo de duda, no es solo la validez de una prueba judicial, si no la definición de la verdad. Si la mente humana se convierte en objeto de análisis computacional ¿que queda del derecho a dudar, a cambiar de idea o incluso a mentir para protegernos? La posibilidad de entrar en el pensamiento antes del acto reabre un viejo problema filosófico ¿Somos realmente libres si todo lo que pensamos puede ser medido y anticipado por una máquina?

Este conflicto entre realidad y lo que percibimos nos recuerda grandes advertencias de la cultura contemporánea. En el show de Truman, la vida del protagonista se desarrolla dentro de una ilusión cuidadosamente diseñada, donde cada pensamiento y emoción son

controlados sin su consentimiento. En la matriz, los seres humanos viven convencidos de una realidad simulada, creada por máquinas que deciden por ellos sobre qué es la verdad y que no. Ambas ficciones ilustran un mismo peligro, cuando el conocimiento se mezcla con el poder absoluto sobre la mente, la libertad se disuelve sin que la persona se de cuenta.

Conclusión

El auge de la Inteligencia Artificial (IA) aplicada a las neurotecnologías particularmente en el procesamiento de señales cerebrales mediante técnicas como fMRI (resonancia magnética funcional), EEG (electroencefalografía) y MEG (magnetoencefalografía)— está abriendo un campo inédito de exploración sobre la actividad neuronal y sus correlatos con procesos cognitivos, emocionales y de memoria. Estas herramientas permiten inferir patrones de activación cerebral que, en teoría, podrían vincularse con pensamientos o intenciones, configurando así un escenario de enorme potencial científico y clínico.

Sin embargo, junto a estas promesas emergen riesgos significativos en materia de privacidad mental, libertad cognitiva y autonomía personal. La posibilidad de acceder, interpretar o incluso modificar información neuronal plantea desafíos éticos y jurídicos sin precedentes. La precisión y el alcance de estos sistemas aún enfrentan limitaciones técnicas, altos costos, sesgos algorítmicos y falta de reproducibilidad, pero las tendencias de desarrollo sugieren que estas barreras podrían ser superadas en un futuro próximo.

En este contexto, se vuelve imprescindible avanzar hacia un marco normativo robusto que regule la captura, almacenamiento y uso de datos neuronales. Chile se ha posicionado como referente global al incorporar los llamados “neuro derechos” en su Constitución, reconociendo la inviolabilidad de la mente y estableciendo salvaguardas contra la manipulación o comercialización de la información cerebral. Este precedente constituye un hito en la protección de la identidad y la integridad mental frente a los riesgos de las tecnologías neurocognitivas.

En Argentina, por el contrario, persiste un vacío legal en torno a estas materias. La falta de regulación específica deja a los ciudadanos potencialmente expuestos a usos indebidos de tecnologías de lectura o interpretación neuronal, especialmente si fueran introducidas en contextos judiciales o de investigación penal. La eventual utilización de registros cerebrales como medios de prueba atentaría contra principios fundamentales consagrados en la Constitución Nacional, particularmente los artículos 16, 18 y 19, que garantizan la igualdad ante la ley, la prohibición de la autoincriminación y la protección de la intimidad.

La introducción de la IA en el ámbito judicial con el propósito de “leer la mente” o inferir estados emocionales del acusado representaría un retroceso ético y jurídico. La justicia no puede reducirse a la precisión técnica de un algoritmo; debe preservar los valores esenciales del Estado de Derecho:

la dignidad, la libertad y la autonomía de la persona.

El desafío del siglo XXI consiste, por tanto, en diseñar marcos éticos y regulatorios sólidos que orienten el desarrollo de la IA y las neurociencias hacia la promoción del bienestar humano, evitando que se conviertan en instrumentos de vigilancia o control mental. La protección del pensamiento y la privacidad neuronal debe entenderse como una extensión contemporánea de los derechos humanos fundamentales.

Bibliografía

Horikawa, T., & Kamitani, Y. (2013). *Decodificación neuronal de imágenes visuales durante el sueño. Science, 340*(6132), 639–642. https://www.science.org/doi/10.1126/science.1234330

Takagi, Y., & Nishimoto, S. (2023). *Reconstrucción de imágenes con modelos de difusión latente desde la actividad cerebral humana. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).* https://arxiv.org/abs/2306.11536

UNESCO Courier. (2023). *Chile pionero en los neuroderechos: ética y regulación de la mente. Revista Altus – Universidad Finis Terrae.* https://bioetica.uft.cl/revista-altus/edicion-no-20/neuroderechos-de-chile-al-mundo/

Congreso de la Nación Argentina. (1994). *Constitución de la Nación Argentina: artículos 16, 18 y 19.* https://www.congreso.gob.ar/constitucionParte1Cap1.php

Analista Programador Universitario egresado de la Universidad Nacional de la Patagonia San Juan Bosco y estudiante avanzado de la Licenciatura en Informática en la misma universidad. Orientado al análisis de datos oceanográficos, el desarrollo de software y la integración de tecnología en trabajos de campo. Experiencia en procesamiento, gestión y visualización de datos ambientales, combinando informática, ciencia y territorio. Con fuerte interés en la investigación científica aplicada y como objetivo profesional consolidarse como buzo científico e investigador, articulando tecnología, datos y ambiente marino.


LEGAL DINOTECH
CONGRESO
EDI
Museo Egidio FERUGLIO
16 y 17 de Abril de 2026
Trelew Chubut

\\EL CENTRO DE FORMACIÓN E INFORMACIÓN MÁS GRANDE DE IBEROAMERICA\\

LA RED

somos

ELDERECHOINFORMATICO.COM