UNIVERSIDAD SIGLO 21

ESPECIALIZACIÓN EN CIBERCRIMEN

¿Cómo es posible detectar, prevenir y mitigar los delitos informáticos contra la integridad sexual de niños, niñas y adolescentes en un contexto de creciente uso de internet y pantallas digitales?

La Inteligencia Artificial aplicada a la detección, prevención y mitigación de delitos contra la integridad sexual de niños, niñas y adolescentes en internet.

ALUMNA: Agusti Yanina.
D.N.I N° 32.157.540
Legajo N° VECB000233

Índice:

Introducción

Según una investigación realizada por UNICEF Argentina sobre las percepciones y hábitos de niños, niñas y adolescentes (en adelante NNA) 8 de cada 10 usaban Internet en el año 2016. (Paolini y Ravalli, 2016, p. 6).[1]

Si bien internet ha posibilitado el desarrollo de las comunicaciones y de la información, también así nuevos escenarios para la comisión de delitos, en particular nos ocupa el grooming on line y la producción, facilitación, comercialización y distribución de material con contenido de abuso sexual de NNA los que, como se explicará más adelante, se encuentran tipificados en nuestro Código Penal a partir de su última reforma.

En un contexto de creciente uso de pantallas digitales y de conectividad a internet, exacerbado por la pandemia COVID-19, estos delitos han aumentado significativamente, exponiendo a NNA a riesgos que afectan su desarrollo neuro psicológico y emocional.

¿Qué políticas públicas y acciones se llevan a cabo para prevenirlos?; ¿Somos conscientes de los profundos daños que quedan en las víctimas? ¿Hablamos y educamos en el uso responsable de las TICs? Comprender los riesgos a los que se enfrentan los NNA en internet es necesario para desarrollar estrategias efectivas de protección que ayuden a salvaguardar a los menores en entornos digitales.

Pese al esfuerzo de organismos e instituciones que persiguen y castigan estas conductas delictivas, se trata de problemática difícil de abordar debido a la vasta cantidad de usuarios, la naturaleza transnacional y el anonimato que los caracteriza. Sin embargo, la Inteligencia Artificial (en adelante IA) puede ser una poderosa herramienta para detectar, prevenir y mitigar estos delitos resultando una especie de guardián en línea, gracias a su capacidad para analizar y procesar grandes volúmenes

[1] Paolini, P., & Ravalli, M. J. (2016). Investigación sobre percepciones y hábitos de niños, niñas y adolescentes en internet y redes sociales. UNICEF. Recuperado de https://www.unicef.org/argentina/media/1636/file/Kids-online.pdf

de datos en tiempo real permite no solo detectar conductas sospechosas, sino también anticipar y actuar ante posibles amenazas, fortaleciendo así la seguridad en el ciberespacio.

Objetivos

El objetivo del presente trabajo es proponer la IA como herramienta para detectar, prevenir y mitigar delitos contra la integridad sexual de NNA en internet.

Para ello se plantean los siguientes objetivos secundarios:

1. Identificar la regulación internacional a la que Argentina suscribe en materia de derechos de NNA y de lucha contra la explotación y abuso sexual de los mismos en internet.

2. Conceptualizar los delitos informáticos contra la integridad sexual de NNA. Análisis de los artículos 128 y 131 del Código Penal.

3. Circunscribir la problemática al entorno local, en el contexto actual y vaticinar a futuro.

4. Distinguir los conceptos de detección, prevención y mitigación.

5. Explicar cómo funciona la IA, el Machine Learning y otras aplicaciones de la IA.

5. Analizar la IA como herramienta para detectar, prevenir y mitigar los delitos informáticos contra la integridad sexual de NNA.

7. Investigar precedentes y nuevas aplicaciones, considerando los beneficios y desafíos para su implementación.

6. Analizar los proyectos de regulación con relación al uso y desarrollo de la IA.

Marco Teórico y Marco Metodológico

Para definir el alcance del presente trabajo y establecer los límites dentro de los cuales se desarrollará, cabe aclarar que abordará exclusivamente los delitos informáticos contra la integridad sexual de NNA. Despleguemos este concepto:

Por niños, niñas y adolescentes (NNA) nos referimos a quienes no han alcanzado la mayoría de edad, es decir menores de dieciocho años conforme lo establece nuestra legislación.

Según la definición publicada en el sitio oficial Mi Argentina, los ciberdelitos o delitos informáticos pueden ser entendidos como todas aquellas conductas ilícitas o antijurídicas que vulneran derechos o libertades de las personas y utilizan un dispositivo informático como medio para la comisión o como fin del delito mismo. (Mi Argentina, 2024).[2]

Aboso señala que existe un consenso en la distinción entre el objeto del ataque y el medio utilizado para cometer delitos informáticos. Si el ataque se dirige contra la integridad o el funcionamiento de un sistema informático, se trata de delitos cibernéticos propios o en sentido estricto; mientras que, cuando una computadora es un medio para llevar a cabo actos ilícitos que afectan bienes jurídicos individuales o colectivos, se habla de ciberdelitos en sentido amplio o impropios. (Aboso, 2020, p. 17).[3]

Los delitos informáticos contra la integridad sexual de NNA, tipificados en nuestro Código Penal en los artículos 128 y 131 son respectivamente el grooming on line y la producción, financiación, oferta, comercialización, publicación, facilitación, divulgación o distribución de material con contenido de abuso sexual de NNA. En este

[2] Mi Argentina (2024). *Delitos informáticos en Argentina.* Jefatura de Gabinete de Ministros de la Nación. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-4

[3] Aboso, G. E. (2020). *DERECHO PENAL CIBERNÉTICO.* Editorial B de F.

trabajo se analizarán por separado las figuras delictivas comprendidas en cada artículo, pero al referirnos a la detección, prevención y mitigación haremos referencia a ambos conjuntamente. Según lo señalado por Aboso, en ambos casos se trata de ciberdelitos en sentido amplio o impropios ya que internet es el medio para la comisión del ilícito.

Por otra parte, el presente tendrá un diseño documental y se apoyará en trabajos desarrollados por autores referentes en la materia, en investigaciones y prototipos previos, como así también los datos recabados por organismos e instituciones serán de importante consideración.

Respecto del marco jurídico se analizará la normativa nacional, los tratados, convenciones internacionales a los que Argentina suscribe en materia de derechos de NNA y ciberdelincuencia, además de los proyectos de regulación de IA.

Así, el Convenio sobre ciberdelito (más conocido como el de Convenio de Budapest) creado en el año 2001 con el objeto de lograr la cooperación internacional en la lucha contra la ciberdelincuencia y ratificado por nuestro país en el 2021, hace referencia a la pornografía infantil, expresión que no utilizaremos como se explicará más adelante. (Convenio de Budapest, 2001, art. 9).[4]

Por su parte, la Convención sobre los Derechos del Niño que Argentina suscribe, establece en sus arts. 19 y 34 el compromiso de los estados parte a proteger al niño contra todas las formas de explotación y abuso sexual. (CDN, 1989, arts. 19 y 34).[5]

La delimitación geográfica o espacial del problema, presenta una dificultad puesto que, por tratarse de delitos cometidos en internet no pueden circunscribirse a un territorio, son transnacionales, es decir traspasan las fronteras de un país y por ende de su sistema normativo. Sin embargo, a los efectos del presente trabajo se tomará como ámbito geográfico de estudio la Provincia de Córdoba y se consultará a las autoridades responsables sobre los casos reportados en los últimos años y si existe, a la fecha, un sistema de IA aplicado a la detección, prevención y mitigación de casos.

Será necesario además, explicar algunos conceptos claves con relación a la IA, el Machine Learning y otras aplicaciones, para luego investigar los precedentes

[4] Convenio de Budapest (2021). *Convenio sobre Ciberdelito*. Ley 27411/2017. Boletín Oficial de la República Argentina.
[5] Ley N° 23849 (1990). *Convención sobre los Derechos del Niño*. Boletín Oficial de la República Argentina.

desarrollados en la detección temprana, prevención y mitigación de delitos de abuso sexual de NNA en plataformas digitales, para finalmente analizar los beneficios y desafíos en su implementación.

Regulación internacional a la que Argentina suscribe en materia de derechos del NNA y lucha contra la explotación y abuso sexual de los mismos en internet.

Convención sobre los derechos del niño.

La Convención sobre los Derechos del Niño, tratado internacional adoptado por la Asamblea General de Naciones Unidas en noviembre de 1989, reconoce a todas las personas menores de 18 años como sujetos de pleno derecho, por ende, el derecho a la integridad sexual. En consecuencia, establece en su art. 34 el compromiso de los estados parte a proteger al niño contra todas las formas de explotación y abuso sexuales y a tomar todas las medidas que sean necesarias para impedir: la incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal, la explotación del niño en la prostitución u otras prácticas sexuales ilegales y la explotación del niño en espectáculos o materiales pornográficos. Argentina ratificó la Convención en el año 1990.[6]

A partir de la reforma constitucional de 1994, por medio del art. 75 inc.22 párr. 2°, se le dio jerarquía constitucional a los tratados y convenciones sobre derechos humanos, entre estos la Convención sobre los Derechos del Niño.[7] Años más tarde, la Ley 26.061 de Protección Integral de los Derechos de la Niñas, Niños y Adolescentes sancionada en 2005 estableció en su art. 2 la aplicación obligatoria de la Convención.[8]

Con el objetivo de asegurar el mejor logro de los propósitos se creó el *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía*, que entró en vigor el 18

[6] Ley N° 23849 (1990). *Convención sobre los Derechos del Niño*. Boletín Oficial de la República Argentina.
[7] Ley N° 24430 (1994). *Constitución Nacional.* Boletín Oficial de la República Argentina.
[8] Ley N° 26.061 (2005). *Protección Integral de los Derechos de la Niñas, Niños y Adolescentes*. Boletín Oficial de la República Argentina.

de enero de 2002. Dicho Protocolo manifiesta la preocupación por el aumento de estas problemáticas y propone un enfoque global con la mirada puesta en los factores que contribuyen, en particular el subdesarrollo, la pobreza, las disparidades económicas, las estructuras socioeconómicas no equitativas, la disfunción de las familias, la falta de educación, la migración del campo a la ciudad, la discriminación por motivos de sexo, el comportamiento sexual irresponsable de los adultos, las prácticas tradicionales nocivas, los conflictos armados y la trata de niños entre otros. (Naciones Unidas, 2000). [9]

El documento, reconoce además, que los NNA son especialmente vulnerables y hace mención a la *Conferencia Internacional de Lucha contra la Pornografía Infantil en la Internet*. (Viena, 1999)

En su art. 2, define el término pornografía infantil como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales" y establece en el art. 3, inc. 1 que todo Estado Parte adoptará medidas para que la producción, distribución, divulgación, importación, exportación, oferta, venta o posesión de pornografía infantil, queden íntegramente comprendidos en cada legislación penal, incluyendo los casos de tentativa. (Protocolo Facultativo de la Convención sobre los Derechos del Niño, 2000, art. 2 y art. 3, inc. 1).[10]

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

Este instrumento fue suscrito en Palermo (Italia) en diciembre de 2000, con la finalidad de promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional. El mismo, reconoce al Gobierno de Argentina por haber acogido la reunión preparatoria del Comité Especial, que se celebró en Buenos Aires, en agosto de 1998.

En su Anexo II incluye un *Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños* cuyo inc. a del art. 3 define "trata de

[9] Naciones Unidas (2000). *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.*
[10] Naciones Unidas (2000). *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.*

personas" a la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. En el inc. c del mismo artículo, establece además que la captación, el transporte, el traslado, la acogida o la recepción de un niño con fines de explotación se considerará "trata de personas" a la vez que en su inc. d agrega que por "niño" se entenderá toda persona menor de 18 años. (Convención contra la Delincuencia Organizada Transnacional, 2000, art. 3).[11]

En agosto de 2002 Argentina aprueba mediante la Ley 25.632 la citada Convención y sus protocolos complementarios.[12]

Convenio de Budapest

El Convenio de Budapest es el primer tratado internacional sobre ciberdelincuencia. Fue elaborado por el Consejo de Europa con la participación de los estados observadores de Canadá, Japón y China; aprobado en el año 2001 pero entró en vigor en el 2004. Dicho acuerdo responde a la necesidad de "… aplicar, con carácter prioritario, una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional…" tal como su preámbulo lo expresa. (Convenio de Budapest, 2001, Preámbulo).[13]

El Convenio tiene particular importancia debido al carácter transnacional de los ciberdelitos, lo que significa que, los delincuentes pueden operar en redes transfronterizas, los servidores pueden encontrarse en cualquier país del mundo y las personas afectadas por estos delitos pueden situarse también en distintos países. El Convenio de Budapest surge ante la necesidad de una armonización legislativa entre las leyes nacionales de cada país, los bloques regionales y los pactos o tratados

[11] Naciones Unidas (2000). *Convención contra la Delincuencia Organizada Transnacional*.
[12] Ley N° 25.632 (2002). *Convención Internacional contra la Delincuencia Organizada Transnacional.* Boletín Oficial de la República Argentina.
[13] Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia*. Preámbulo.

internacionales, como así también la cooperación entre los países para perseguir este tipo de delitos. El instrumento se compone de 48 artículos distribuidos en 4 capítulos.

El Capítulo I contiene las definiciones de “sistemas informáticos”, “datos informáticos”, “proveedor de servicios” y “datos relativos al tráfico”.

Por su parte, el Capítulo II detalla las medidas que deben en caso de infracciones contra la confidencialidad, contra la integridad, disponibilidad de datos y sistemas informáticos, delitos relacionados con la pornografía infantil y relacionados con infracciones de la propiedad intelectual y de derechos afines. También establece medidas sobre cómo se debe llevar a cabo el procedimiento de investigación y determina ciertas disposiciones procesales y acciones referidas a la obtención e interceptación de datos.

El Capítulo III abarca los principios generales relativos a la cooperación internacional, la asistencia mutua y la comunicación entre los Estados parte.

Finalmente, el Capítulo IV contiene las “Cláusulas Finales” con relación a la firma y a la entrada en vigor del Convenio, el proceso de adhesión al mismo, la delimitación de la aplicación territorial y la posibilidad de cada Estado parte de realizar declaraciones, proponer enmiendas o adherir a las reservas previstas al momento de incorporarse al Convenio.

De especial interés para el tema que nos ocupa es el artículo 9 del Capítulo II, sobre “delitos relacionados con la pornografía infantil”, el cual reza:

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

   a. La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

c. La difusión o transmisión de pornografía infantil a través de un sistema informático;

d. La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;

e. La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos".[14]

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:
   a. un menor adoptando un comportamiento sexualmente explícito.
   b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito.
   c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.[15]
3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.[16]
4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.[17]

Luego de la entrada en vigor del Convenio, el Consejo de Europa convocó a la adhesión de países no miembros que no hubieran participado en su elaboración. En

[14] Art.9 Inc.1 Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia*.
[15] Art.9 Inc.2 Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia.*
[16] Art.9 Inc.3 Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia.*
[17] Art.9 Inc.4 Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia.*

consecuencia, el 4 de junio de 2008 en nuestro país adhirió y se sancionó la Ley N.º 26.388 conocida como Ley de Delito Informático que modificó el Código Penal Argentino, tipificando las conductas delictivas vinculadas con la ciberdelincuencia en base a lo establecido en el Convenio y modificó el artículo 77 del Código Penal respecto de los significados y usos conceptuales ampliados de los términos "documento", "firma digital", "suscripción", "instrumento privado" y "certificado" (Ley 26.388, 2008, art. 1°).[18]

Dicha ley, también modificó el art. 128 del CP estableciendo:

> ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:
>
> Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
>
> Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años. (Ley 26.388, 2008, art. 2°).[19]

[18] Ley N° 26.388 (2008). *Delitos Informáticos y Ciberseguridad.* Boletín Oficial de la República Argentina.
[19] Ley N° 26.388 (2008). *Delitos Informáticos y Ciberseguridad.* Boletín Oficial de la República Argentina.

Como puede observarse, las actividades simuladas fueron excluidas, como así también así la simple posesión.

En marzo de 2010 se desarrolló la Conferencia sobre Cooperación contra el Cibercrimen, organizada por el Consejo de Europa en la ciudad de Estrasburgo y fue entonces que Argentina presentó su solicitud para acceder a la Convención de Budapest. Años más tarde, el 22 de noviembre de 2017 la Honorable Cámara de Diputados de la Nación aprobó la Ley N° 27.411 de ratificación de la Convención de Budapest, mediante la cual se produjo la adhesión de nuestro país a dicho instrumento con algunas reservas, entre estas, la reserva parcial del artículo 9.1.e. del Convenio sobre Ciberdelito que, como ya nos hemos referido, refiere a la simple tenencia entendiendo por esta "la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos" (Convenio de Budapest, 2001, art.9 Inc.1.e).[20]

En este sentido, Argentina argumentó que la simple tenencia no regiría en su jurisdicción por entender que, según la legislación penal vigente hasta la fecha, sólo es aplicable cuando la posesión referida fuera cometida con inequívocos fines de distribución o comercialización tal como quedara la redacción del artículo 128, segundo párrafo, del Código Penal modificado por la Ley N.º 26.388 (Ley N.º 26.388, 2008, art. 2 segunda parte).[21]

Sin embargo, tal como explica Riquert, el mismo legislador apenas tres meses después decidió incorporar como nuevo segundo párrafo al C.P. la propuesta de conducta típica de la que había hecho reserva mediante el art. 1° de la ley 27.436 y completó la reacción vigente con el siguiente agregado: "Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior" (Riquert, 2020, p. 98).[22]

Así también, nuestro país hizo reserva del art. 9.1.d. y del 9.2 en los puntos b y c.

[20] Art.9 Inc.1.e Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia*.
[21] Art. 128, segundo párrafo, del Código Penal modificado por la Ley N.º 26.388/2008. Boletín Oficial de la República Argentina.
[22] Riquet, Fabián Luis (2019). *CIBERDELITOS*, Capítulos VII. Editorial Hammurabi.

Delitos informáticos contra la integridad sexual de niños, niñas y adolescentes. Análisis de los artículos 128 y 131 del Código Penal.

> «Si puedes claramente y consistentemente nombrar y definir un delito, esto contribuye a la prevención y lucha contra ese delito. Esto ha demostrado ser muy importante en la lucha contra la explotación sexual infantil y el abuso sexual. La falta de un lenguaje común ha contribuido a las deficiencias de los esfuerzos mundiales para proteger a los niños.» (Mezmur, 2016).[23]

Para abordar de manera efectiva la detección, prevención y mitigación de los delitos informáticos contra la integridad sexual de NNA, es fundamental primero definir estos delitos. Esto implica el análisis de la acción antijurídica (es decir el comportamiento que viola la ley), de la conducta típica (que se refiere a las acciones concretas que constituyen el delito según la legislación vigente) y del bien jurídico protegido (que en ambos casos se trata de la integridad sexual de NNA, un derecho fundamental cuya protección es prioritaria).

Este análisis no solo permite identificar con precisión las amenazas y vulnerabilidades a las que se enfrentan los NNA en el entorno digital, sino que también proporciona una base sólida para desarrollar estrategias de detección, prevención y mitigación efectivas. Nuestro Código Penal refiere a las conductas reprochables de abuso mediante la producción, financiación, oferta, comercialización, publicación, facilitación, divulgación o distribución de toda representación sexual de NNA en su art. 128 y al grooming online en su art. 131 aunque, como ya veremos, sin llamarlo de ese modo.

Analicemos entonces cada figura y su regulación:

---

[23] Mezmur, B. D. (2016). *Las directrices lingüísticas son una herramienta clave para abordar el abuso sexual infantil.* Organización de las Naciones Unidas. Recuperado de https://www.ohchr.org/en/press-releases/2016/06/language-guidelines-key-tool-tackling-child-sex-abuse-un-child-rights

Artículo 128 del Código Penal.

Como se mencionó anteriormente, el delito de "pornografía infantil" a la que refiere el art. 9 del Convenio de Budapest fue incorporado al art. 128 de nuestro Código Penal mediante la Ley 26.388. Esta incorporación representó un paso significativo para alinear de la legislación nacional con los estándares internacionales en la lucha contra los delitos que afectan la integridad sexual de NNA. Posteriormente, fue modificado por la Ley N° 27.436, para adaptarlo a las nuevas realidades tecnológicas y a los compromisos internacionales asumidos por el país. El artículo reza:

> Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.
>
> Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.
>
> Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.[24]

Las principales diferencias del artículo modificado por la Ley N° 27.436 respecto del anterior son:

- Se incorporó en el segundo párrafo el delito de tenencia simple.
- Se aumentó la pena de las conductas descritas en el primer párrafo tanto en el mínimo como en el máximo.
- Respecto del antiguo segundo párrafo (actual tercero) se aumentó solo el mínimo que antes era de cuatro meses, modificándose a seis meses de prisión.
- Se estableció un agravante genérico para todos los delitos tipificados en el artículo cuando la víctima es menor de trece años.

Respecto del bien jurídico protegido, tal como explica Aboso, en su redacción original tuvo como propósito tutelar una moralidad sexual determinada, pero la Ley 25.087 introdujo un cambio radical en la orientación político-criminal de la norma al focalizarse en la tutela de los menores de edad dejando de lado los resabios de una moralidad pública (Aboso, 2020, p.202).[25]

En el mismo sentido, completa Riquert, explicando que el bien jurídico que se pretende tutelar es el normal desarrollo psíquico y sexual de quienes no han alcanzado la edad de 18 años y por ende la suficiente madurez. (Riquert, 2020 p. 262). [26]

El artículo establece en sus párrafos distintos tipos penales utilizando una sucesión de verbos con los que el legislador procura alcanzar como refiere el autor, todo lo que configuraría la cadena de elaboración y comercialización de la pornografía infantil: producir, financiar, ofrecer, suministrar, comerciar, publicar, facilitar, divulgar y distribuir. Respecto del segundo párrafo que refiere a la simple tenencia, genera

[24] Art. 128 Código Penal, modificado por Ley N° 27.436 (2018). Boletín Oficial de la República Argentina.
[25] Aboso, G. E. (2020). *DERECHO PENAL CIBERNÉTICO.* Editorial B de F.
[26] Riquet, Fabián Luis (2019). *CIBERDELITOS*, Capítulos VII. Editorial Hammurabi.

controversia ya que algunos sostienen que, juzgar esta conducta implicaría una intromisión en el ámbito de la privacidad (Riquert, 2020 p. 262).[27]

El sujeto pasivo es todo menor de 18 años con relación a la primera parte de la norma mientras que, en el último párrafo, desciende a 13 años respecto a menores a los que se les facilitare el acceso a espectáculos pornográficos o se les suministrare material pornográfico. Por otra parte, el sujeto activo es cualquier persona que realice las conductas establecidas en la norma, y no ha contemplado agravante por la calidad de autor (padre, tutor, curador).

Como analiza Riquert, se trata de un tipo penal doloso, no sólo directo sino con posible dolo eventual, toda vez que no existe la figura culposa, mientras que el párrafo 2° sólo admite el dolo directo y en el 3° se verifica la exigencia de una ultra intencionalidad ya que la tenencia demanda que sea con fines inequívocos de distribución y comercialización (Riquert, 2020 p. 262).[28]

Todas las conductas descriptas por la norma admiten la tentativa sin perjuicio de tratarse, en la mayoría de los verbos típicos, de un delito de mera actividad excepto la publicidad establecida en el primer párrafo, donde el delito se consuma una vez realizada las tomas o filmaciones sin necesidad de que se acredite su divulgación ya que, lo que se protege es la indemnidad sexual y dignidad de los menores, explica también el autor (Riquert, 2020 p. 269).[29]

Como se puede advertir, el artículo no incorpora en su redacción la expresión “pornografía infantil” a la que se refiere el Convenio de Budapest, toda vez que este término genera controversia.

Al respecto, un grupo de expertos internacionales junto a la Organización ECPAT (End Child Prostitution, Child Pornography and Taffiking of Children for Sexual Purposes que en español significa Acabar con la Prostitución Infantil, la Pornografía Infantil y el Tráfico de Niños con fines Sexuales) crearon en Luxemburgo, una serie de directrices sobre el uso del lenguaje con relación al abuso y la explotación sexual de NNA. Estas, que se conocen como las *Directrices de Luxemburgo*, recomiendan la utilización de la

[27] Riquet, Fabián Luis (2019). *CIBERDELITOS*, Capítulos VII. Editorial Hammurabi.
[28] Riquet, Fabián Luis (2019). CIBERDELITOS, Capítulos VII. Editorial Hammurabi.
[29] Riquet, Fabián Luis (2019). CIBERDELITOS, Capítulos VII. Editorial Hammurabi.

expresión "*material de abuso sexual infantil",* en adelante CSAM (por sus siglas en inglés de *child sexual abuse material*) en reemplazo de la expresión pornografía infantil ya que esta última, puede llevar a admitir distintas interpretaciones y generar confusión. Los expertos explican que, la pornografía es cada vez más aceptada socialmente, pero este término utilizado con relación a los NNA puede (de forma involuntaria o voluntaria) contribuir a disminuir la gravedad, normalizar o incluso legitimar lo que en realidad se trata de abuso sexual de NNA (ECPAT International, 2016, p. 44).[30]

En este sentido, la doctrina es unánime al entender que el término "pornografía" alude a la representación de actos sexuales o eróticos consensuados, destinados a provocar excitación sexual o placer. Pero cuando se trata de NNA, no se puede hablar de actos consensuados por su incapacidad para discernir y elegir libremente. Esta incapacidad implica que cada imagen o representación de estos actos constituye un abuso en sí mismo.

Por lo tanto, para referirse a imagen o representación de estos actos que involucran a NNA, es preciso utilizar la expresión "abuso sexual de niñas, niños y adolescentes" en lugar de "pornografía infantil" ya que esta última locución no refleja adecuadamente la gravedad del delito y puede llevar a interpretaciones erróneas lo que podría resultar en una distorsión o minimización del fenómeno que describe.

En consecuencia, al abordar casos que involucran a NNA, es fundamental usar un lenguaje que refleje con precisión la naturaleza del delito. La expresión "abuso sexual de niñas, niños y adolescentes" no solo describe con exactitud la gravedad del acto, sino que también contribuye a una comprensión más adecuada y respetuosa del sufrimiento de las víctimas y la necesidad de una respuesta legal y social apropiada.

La terminología precisa no solo es importante para el correcto entendimiento de la conducta antijurídica, sino también para garantizar que se brinde el adecuado apoyo y justicia a las víctimas, a la vez que se trabaje mancomunadamente para desarrollar políticas estratégicas de detección, prevención y mitigación de estos delitos.

---

[30] ECPAT International (2016) *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.* Recuperado de https://ecpat.org/luxembourg-guidelines/

Artículo 131 del Código Penal.

En el año 2013, la Ley N° 26.904 incorporó el ciberacoso o grooming on line al Código Penal cuyo art. 131 reza:

> Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. (Ley N.º 26.904, 2013, art. 131). [31]

Miriam C. Mauri explica que, en la decisión de legislar sobre esta figura, confluyeron varios motivos: por un lado, la voluntad de afianzar la protección de los menores que no han alcanzado la edad de la madurez sexual y por el otro la necesidad de reforzar la tutela penal de ese bien jurídico ante el riesgo del uso de las tecnologías de la información y comunicación (TIC). (Mauri, 2019, p. 234).[32]

El grooming on line refiere entonces a toda forma de acoso, manipulación, persecución o cualquier conducta de facilitación que un adulto despliega respecto de un menor de edad a través de plataformas digitales (como redes sociales, mensajería instantánea, correos electrónicos o juegos on line) con un propósito o finalidad sexual.

Implica una serie de conductas intencionales con el objetivo de ganarse la confianza del NNA y se caracteriza por ser un proceso gradual y meticuloso, donde el adulto explota las vulnerabilidades del menor para cumplir sus objetivos ilícitos.

La Organización GROOMING ARGENTINA fue creada en el año 2014, tras la incorporación y tipificación de este delito en el Código Penal Argentino, con el propósito de trabajar fundamentalmente en la prevención y concientización en pos de la erradicación del grooming.

---

[31] Ley N° 26.904. (2013). *Modificación del Código Penal e incorporación del artículo 131 sobre ciberacoso o grooming.* Boletín Oficial de la República Argentina.
[32] Mauri, Miriam C. (2019). *CIBERDELITOS*, Capítulos VI. Editorial Hammurabi.

La Organización, explica en su sitio web, que Grooming on line implica un proceso que consta de distintas etapas e incluye una serie de conductas que pueden o no seguir el mismo orden, pero por lo general existen patrones comunes que podemos resumir en:

1. Etapa de enganche o entrapment (atrapamiento): con el objetivo de acercarse a la víctima y ganar su confianza la persona adulta, a través de un perfil falso, finge otra identidad generalmente de edad muy cercana toma contacto y establece un vínculo de amistad con un NNA. Ganando su confianza logra obtener más información, puede que empatice escuchando sus problemas y aproveche esa información para chantajearlo después.

2. Etapa de fidelización: en esta etapa el acosador con la información que conoce del niño, niña o adolescente intentará mantener cautiva su atención a través del intercambio de secretos, confidencias, promesas, etc. El agresor se propone apartar al NNA de su círculo (familiares, amistades, docentes, etc.) para dejarlo desprotegido.

3. Etapa de seducción: el agresor empieza a introducir conversaciones sexuales de manera paulatina generalmente mediante preguntas y/o relatos, para generar en el niño, niña o adolescente un compromiso y/o dependencia emocional.

4. Etapa de acoso sexual: Esta etapa se caracteriza por una marcada agresión sexual, implícita o explícita, en la cual el acosador manipula a la víctima a través de la solicitud de imágenes y/o videos íntimos, o bien, la propuesta de un encuentro personal. En aquellos casos en los cuales el niño, niña o adolescente no acceda a sus requerimientos, el acosador ejercerá distintas formas de violencia, tales como: chantaje, extorsión, amenazas o coacciones para que la víctima le envíe material sexual, relate fantasías sexuales o la relación culmine con un encuentro físico.[33]

El adulto, aprovechando la situación de indefensión, genera un vínculo emocional con el NNA a fin de disminuir sus inhibiciones para luego lograr su cometido que puede

[33] Grooming Argentina. *¿Qué es el grooming?* Recuperado de https://www.groomingarg.org/

ser desde obtener material con contenido sexual de la víctima para su comercialización, distribución y/o para satisfacer su perversión sexual hasta incluso ser generar un encuentro personal.

La figura de Grooming se caracteriza entonces por: la conducta desplegada de un adulto respecto de un menor, la particularidad del medio utilizado, la finalidad sexual que persigue el autor. La acción típica de la conducta delictiva implica que el adulto establezca un contacto con el menor con la finalidad específica de inducirlo a realizar actos de naturaleza sexual (Riquert, 2020 p. 246).[34]

En el art. 131 del Código Penal, el bien jurídico tutelado es también la integridad sexual y el normal desarrollo psico biológico sexual de los NNA toda vez que no han alcanzado la madurez, como ya se ha explicado anteriormente. El sujeto pasivo entonces es todo menor de dieciocho años mientras que el sujeto activo puede ser cualquier persona que realice la conducta descripta en la norma.

Se trata de un delito doloso compatible con la figura del dolo directo. El art. 131 demanda que la conducta desplegada por el autor haya sido con discernimiento, intención y voluntad. El dolo directo implica que el autor del delito tiene un objetivo específico de lograr que el menor realice o participe en actividades sexuales. La intención del adulto es deliberada y no deja lugar a interpretaciones ambiguas sobre su propósito. En cuanto a si es considerado un delito continuado, la jurisprudencia y la doctrina no son unánimes. Parte interpreta que sí debido a que implica un proceso de acercamiento y manipulación prolongada en el tiempo mientras que otra parte sostiene que cada acto de contacto con el menor podría constituir un delito separado.

Con el aumento del uso de dispositivos electrónicos desde edades cada vez más tempranas y la creciente exposición de NNA a internet, el grooming online ha emergido como una nueva forma de abuso sexual sin contacto físico. Este fenómeno representa una problemática cada vez más alarmante.

Ley 27.590 “Mica Ortega”

[34] Riquet, Fabián Luis (2019). CIBERDELITOS, Capítulos VII. Editorial Hammurabi.

En abril de 2016, Micaela Ortega una niña de 12 años, fue asesinada tras ser engañada a través de Facebook por un hombre que, detrás de un falso perfil fingió tener la misma edad y captar su amistad. Micaela salió de su casa rumbo a un encuentro con su nueva amiga, pero nunca regresó. Pese a los rastrillajes y operativos para dar con la niña, los resultados fueron negativos. La búsqueda para dar con su paradero rápidamente se viralizó en los medios de comunicación. Sin embargo, ya había transcurrido un mes y Micaela continuaba desaparecida. Su búsqueda se sumó al National Center for Missing & Exploited Children y a partir de los datos aportados, los investigadores dieron con Jonathan Luna, un hombre de 26 años y que había contactado a Micaela a través de la red social. La Justicia ordenó el allanamiento de su vivienda y allí encontraron el celular y la campera de la menor. El hombre fue detenido y terminó confesando que había asesinado a Micaela y reveló el lugar de donde había escondido el cuerpo (Infobae, 2024).[35]

A raíz de este hecho aberrante, en 2020 se sancionó la Ley 27.590, llamada también Ley Mica Ortega que en su art. 3º establece que, por grooming o ciberacoso se entiende la acción en la que una persona por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a una persona menor de edad con el propósito de cometer cualquier delito contra la integridad sexual de la misma (Ley 27.590, 2020, art.3).[36]

El 14 de julio de 2022, el Poder Ejecutivo Nacional emitió el Decreto Reglamentario 407/2022, que aprobó la reglamentación de la Ley “Mica Ortega”

La Ley y su Decreto 407/2022 de reglamentación crearon el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes cuyos objetivos, conforme establece la norma son:

a) Generar conciencia sobre el uso responsable de las Tecnologías de la Información y Comunicación.

[35] Infobae. (2024). *El crimen de Micaela Ortega, la nena de 12 años cuyo caso impulsó la ley de grooming.* Recuperado de *https://www.infobae.com/sociedad/2021/08/04/el-crimen-de-micaela-ortega-la-nena-de-12-anos-cuyo-caso-impulso-la-ley-de-grooming/*

[36] Ley N° 27.590. (2020). *Ley Mica Ortega sobre la prevención y concientización del ciberacoso o grooming.* Boletín Oficial de la República Argentina.

b) Garantizar la protección de los derechos de las niñas, niños y adolescentes frente al grooming o ciberacoso.

c) Capacitar a la comunidad educativa en el nivel inicial, primario y secundario de gestión pública y privada a los fines de concientizar sobre la problemática del grooming o ciberacoso.

d) Diseñar y desarrollar campañas de difusión a través de los medios de comunicación masiva a los fines de cumplir con los objetivos del presente Programa.

e) Brindar información acerca de cómo denunciar este tipo de delitos en la justicia. (Ley 27590, 2020, art. 4°).[37]

El caso de "Mica Ortega" marcó un hito significativo en la historia judicial de Argentina, ya que Jonathan Luna fue condenado a prisión perpetua en el primer juicio por grooming seguido de muerte en el país. Pero seguramente Micaela no fue la única víctima, ni Luna el único agresor en aquel entonces.

La Ley 27.590, junto con el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra NNA, ha sido un avance en la lucha contra este delito. La ley establece un marco legal para la identificación y sanción del grooming, mientras que el programa busca sensibilizar y promover estrategias de prevención. No obstante, pese a estos importantes pasos hacia adelante, aún persisten desafíos significativos. Solo a través de un enfoque integral y coordinado se podrá enfrentar adecuadamente este delito y proteger a los menores en el entorno digital.

Una problemática actual. Una problemática real.

[37] Ley N° 27.590. (2020). *Ley Mica Ortega sobre la prevención y concientización del ciberacoso o grooming.* Boletín Oficial de la República Argentina.

Las víctimas de estos delitos son especialmente vulnerables toda vez que afecta a su desarrollo neuropsicológico, funcionamiento sexual y puede desencadenarse trastornos ya que, como explica Gemma Mestre, los niños se encuentran en un estadio evolutivo en proceso, tanto a nivel físico y emocional como cognitivo, es decir que los procesos de madurez están inconclusos, por ende, separar realidad de ficción les cuesta mucho más. (Gemma et al, 2023, p.12).[38]

En otras palabras, la exposición a situaciones de abuso sexual en línea sin duda tiene un impacto profundamente negativo en el desarrollo mental y emocional de la víctima, con consecuencias graves y duraderas. Los NNA que sufren este tipo de abuso a menudo enfrentan sentimientos como miedo, culpa, impotencia, desamparo y vergüenza. Estos sentimientos pueden llevar a que las víctimas permanezcan en silencio, ocultando su sufrimiento y afectar severamente su bienestar psicológico y su capacidad para desarrollarse de manera saludable.

La infancia y el desarrollo pleno son derechos protegidos internacionalmente, así lo refiere el art. 27 de la Convención sobre los Derechos del Niño que establece el derecho a un nivel de vida que le permita su desarrollo físico, mental, espiritual, moral y social. (CDN, 1989, art. 27) [39]

Sin embargo, a diario se difunden miles de imágenes y vídeos a través de internet en los que NNA son víctimas de abuso sexual y en diferentes partes del mundo y a cada hora, un menor está siendo contactado por un adulto con un propósito o finalidad sexual.

La preocupación sobre estos delitos quedó instalada en nuestro país a partir del caso Mica Ortega y de los resultados de la llamada *Operación Ángel Guardián* que, en ese mismo año (2016) permitió desarticular las actividades de otro ciberacosador que había extorsionado al menos a 43 víctimas menores de edad.

La investigación fue iniciada por el MPF de Bs. As. pero, dada la cantidad de víctimas afectadas en diferentes provincias debió intervenir el Consejo de

---

[38] Giulia Testa, Alejandro Villena, Gemma Mestre y Carlos Chiclana. (2023). *Guía para familias adolescentes y uso de pornografía.* UNIR. Recuperado de https://www.unir.net/wp-content/uploads/2023/12/Guia-para-Familias_Adolescentes-y-Uso-de-Pornografia.pdf

[39] Convención sobre los Derechos del Niño. (1989). UNICEF Comité Español.

Procuradores, Fiscales y Defensores Generales de la República Argentina. La operación se organizó luego de advertir el ingreso de gran cantidad de reportes NCMEC (National Center Missing and Exploited Children) que seguían un patrón común, surgiendo luego otros usuarios receptores de dichas imágenes con distintas identidades pero que utilizaban la misma dirección IP, circunstancia que permitió sospechar que se trata del mismo usuario.

El ciberacosador, empleando varios perfiles falsos generados en la red social Facebook se contactaba con niñas de entre 12 y 16 años y luego de entablar un vínculo de confianza, las manipulaba o extorsionaba para que le enviaran fotografías y videos con el cuerpo total o parcialmente desnudo, en posiciones y/o actitudes explícitamente sexuales, que eran expresamente indicadas por el agresor.[40]

Son varios factores que confluyen y que hacen de esta, una problemática actual y real. Incluso se vaticina un crecimiento exponencial si no se toman las acciones necesarias para detectar, prevenir y mitigar estos delitos.

El primer factor es el tecnológico. Gustavo E. Aboso afirma que el desarrollo tecnológico trajo consigo un efecto negativo que lamentablemente se cristaliza en la irrupción de nuevas formas de comportamientos que atentan contra la integridad sexual de los menores de edad. (Aboso, 2020, p.237).[41]

El uso de tecnologías de la información y de las comunicaciones digitales (TICDs) se incrementó exponencialmente a nivel global durante los últimos años. Es probable que la pandemia COVID-19 y las medidas de confinamiento dispuestas para evitar la propagación de la enfermedad hayan incidido Durante la pandemia, los NNA exploraron nuevas formas de socializar mediante juegos, chats o redes sociales. El teletrabajo, la educación a distancia y las compras on line se volvieron habituales. Estás nuevas dinámicas de conectividad llegaron para quedarse.

Un informe a cargo de la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, sobre los ciberdelitos en Argentina durante la pandemia del COVID-19, puso de manifiesto la incidencia de este contexto: en el año 2020 se

[40] Centro de Información Jurídica. (2016). *Operación Ángel Guardián.* Ministerio Público Provincia de Buenos Aires. Recuperado de https://www.mpba.gov.ar/novedad/515

[41] Aboso, Gustavo Eduardo (2020). *DERECHO PENAL CIBERNÉTICO*. Capítulo VI: CHILD GROOMING. Editorial B de F.

receptaron en nuestro país un total de 4.446 denuncias sobre tenencia, distribución o publicación de imágenes de abuso sexual de NNA (art. 128 C.P.) y 1.751 denuncias sobre grooming (art. 131 C.P.) ascendiendo estos números a 4.526 y 1.878 respectivamente en el año 2021 (Carnaghi Cintia et al, 2022, p. 33). [42]

Un desglose por provincia en dicho informe muestra que, del número total referido anteriormente, en la provincia de Córdoba se receptaron 70 denuncias respecto del Art. 128 CP y 84 respecto del Art. 131 CP. A continuación, se puede apreciar el porcentaje que representan ambas figuras con relación al resto de los ciberdelitos denunciados en el mismo año:

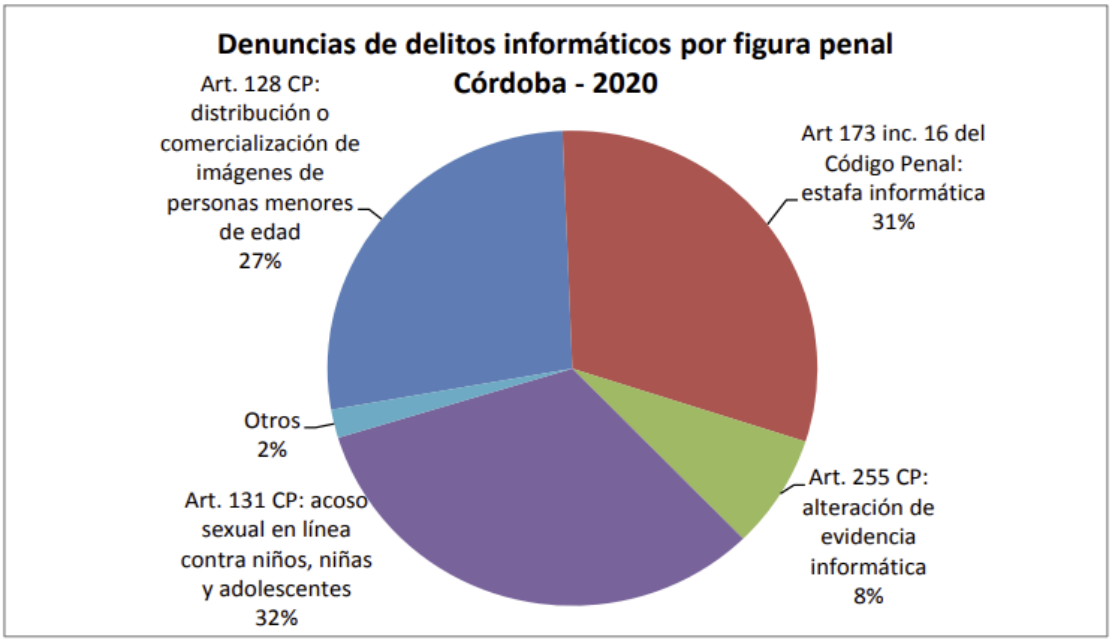

Figura 1: Ciberdelitos denunciados en Córdoba – 2020

Al año siguiente, se registraron en nuestra provincia 85 denuncias respecto del Art. 128 CP y 92 respecto del Art. 131 CP. A continuación, se puede apreciar le porcentaje que representan ambas figuras respecto del resto de los ciberdelitos denunciados en el mismo año:

[42] Carnaghi Cintia et al. (2022). *Ciberdelitos durante la pandemia del covid-19 en Argentina.* Ministerio de Justicia y DD. HH de la Nación.

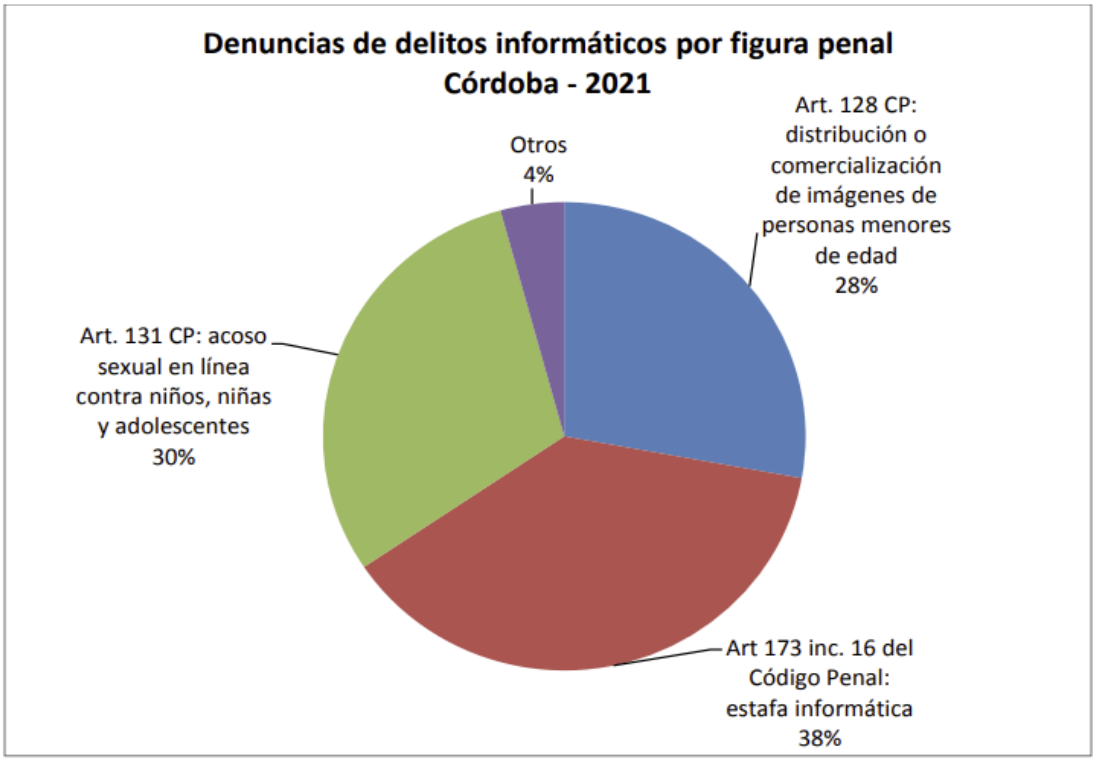

Figura 2: Ciberdelitos denunciados en Córdoba – 2021

Por otra parte, entrevistado personal de la Oficina de Ciberdelitos del Ministerio Público Fiscal de Córdoba refirió que en el año 2019 se iniciaron 47 causas por hechos vinculados a delitos informáticos contra la integridad sexual de NNA, sin poder especificar exactamente cuántas corresponden al Art. 128 CP y 92 y al Art. 131 CP.[43]

Este número da cuenta de que en el año 2019 se registraron significativamente menos denuncias en comparación con 2020 y 2021.

La misma Oficina del Ministerio Público Fiscal de Córdoba registró un total de 415 casos en el año 2022 con una leve baja a 329 en 2023.[44]

Otro factor que contribuye al aumento de estos delitos es la creciente tendencia al uso de dispositivos electrónicos y la conectividad a Internet a edades cada vez más tempranas.

En febrero de 2020 UNICEF presentó los resultados de un relevamiento que realizó en nuestro país sobre el uso de la tecnología y la seguridad en línea. La agencia

[43] Oficina de Ciberdelitos. (2024). Ministerio Público Fiscal de Córdoba.
[44] Oficina de Ciberdelitos. (2024). Ministerio Público Fiscal de Córdoba.

encuestó a un total de 560 jóvenes de 13 a 18 años y los datos fueron relevados en canales digitales a través de la plataforma U-Report. Los resultados arrojados demuestran que 9 de cada 10 adolescentes ingresan a Internet a través del celular, que 13 años es la edad promedio en la que recibieron su primer dispositivo con conexión a Internet y que el 50% de los y las adolescentes experimentó una situación negativa en la red (Unicef, 2020). [45]

Según un informe publicado por la consultora Statista Research Department sobre el porcentaje de la población con acceso a Internet en Argentina, realizado a través de encuestas en diferentes ciudades del país entre octubre y diciembre de 2022, el 81,5% de los NNA de 4 a 12 años tenía acceso a Internet, mientras que del grupo muestra de 13 a 17 años el porcentaje era de 95,7%. (Statista Research Department, 2024).[46]

Estos resultados dan cuenta de que, en la actualidad, la mayoría de los NNA tienen acceso a dispositivos electrónicos y a internet. Miles de pederastas ven esto como un escenario positivo para captar a más víctimas y aprovechándose de su vulnerabilidad, logran manipularlos para conseguir un objetivo de índole sexual.

Como se mencionó anteriormente, los NNA pueden estar expuestos a peligros incluso en los juegos en línea. Aunque existen restricciones de edad, la falta de una verificación efectiva posibilita a que muchos jóvenes accedan a foros o chats de adultos, se expongan a contenidos violentos o inapropiados, incluso este es un escenario que los pederastas aprovechan para contactar a NNA, por lo que también pueden ser víctimas de grooming.

En sus Directrices de Protección de la Infancia en Línea para la Industria (2015), UNICEF recomienda cinco acciones que las compañías de tecnología deben hacer para proteger a los NNA que utilizan sus servicios:

1.Los derechos de los niños deben integrarse en todas las políticas y procesos correspondientes de la compañía.

[45] Unicef (2020). *Google y UNICEF revelan cuáles son las preocupaciones de adolescentes, familias y docentes sobre el uso de la tecnología*.
[46] Statista Research Department. (2024). *Argentina: porcentaje de población con acceso a internet, por edad 2023.*

2.La compañía debe haber incorporado procesos para lidiar con las violaciones a los derechos de los niños.

3.Los medios que ofrecen las compañías tienen que ser apropiados de acuerdo a la edad.

4.La compañía debe educar a los niños, a sus padres y a sus cuidadores respecto a cómo usar los productos de manera responsable.

5.La tecnología digital debe promoverse como un medio para aumentar la participación cívica (UNICEF, 2015, p. 6-12).[47]

El anonimato, que caracteriza el uso de internet, favorece la comisión de delitos y este es otro importante factor. No es suficiente con detectar material con contenido de abuso sexual infantil y eliminarlo, también es clave para la justicia identificar a los autores y juzgarlos.

Para dar con los autores, la dirección de IP podría ser de gran ayuda. Cuando un dispositivo se conecta a una red, se produce un intercambio de datos entre la computadora y el proveedor que permite individualizar la información de quien contrató el servicio de internet con el proveedor y así obtener la dirección del domicilio donde se encuentra el terminal, lo que no significa que quien contrata el servicio sea el mismo usuario que se conecta.

Sin embargo, puede ocurrir que el usuario utilice programas para interferir o impedir la determinación de la dirección de IP como el sistema TOR, o que use IP dinámicas, redes abiertas públicas o privadas con acceso a terceros para no ser identificado.

Otro factor determinante es que se trata de delitos transnacionales, es decir que trascienden las fronteras de un país, por ende, de su sistema normativo. Esta cuestión es verdaderamente importante ya que, no todos los países han suscripto a los tratados

[47] Unicef (2015). *Directrices de Protección de la Infancia en Línea para la Industria.* Recuperado de https://www.unicef.org/dominicanrepublic/media/916/file/Publicaci%C3%B3n%20%7C%20Directrices%20de%20proteccion%20de%20la%20infancia%20en%20linea%20para%20la%20industria.pdf

y convenciones internacionales en materia de ciberdelitos y delincuencia organizada transnacional, sumado a que el grado de desarrollo alcanzado es diferente y las culturas heterogéneas. De este modo un agresor puede encontrarse en un país, utilizar los servidores de otro y captar un NNA de otra parte del mundo lo que dificultaría la trazabilidad del delito y dado que las políticas de seguridad y la legislación son diferentes en cada uno, eludir ser juzgado. La cooperación internacional en la lucha contra los delitos transnacionales, especialmente aquellos relacionados con el abuso infantil y el material de explotación sexual, se ha vuelto crucial en la era digital.

En este sentido, la IWOL List de INTERPOL es una herramienta para la cooperación entre diferentes países y agencias en la lucha contra estos delitos ya que proporciona una base de datos común sobre dominios de internet que han sido identificados como peligrosos y asociados con actividades delictivas relacionadas con la explotación sexual infantil, lo que permite monitorearlos incluso desmantelar sitios web que albergan, distribuyen o intercambian material de abuso sexual infantil.

Por último, la diferencia generacional entre los NNA por un lado y los padres, tutores y educadores por el otro, puede considerarse un factor si se tiene en cuenta que muchos adultos desconocen, incluso ignoran esta problemática.

Como se refirió antes, estamos viviendo tiempos de rápida transformación digital y los adultos a menudo muestran una fuerte reticencia a los cambios. Los maestros, padres y cuidadores deben tener al menos los conocimientos y habilidades digitales básicas para aprovechar los beneficios de estar conectados, pero también reconocer y responder de manera adecuada frente a cualquier amenaza. Los filtros parentales son herramientas de mucha utilidad para bloquear sitios o filtrar contenidos, pero de ningún modo puede reemplazar el acompañamiento físico de personas adultas que a partir del diálogo fomenten una mirada crítica y reflexiva

Para proteger a los NNA en línea, es necesario comprender los riesgos a los que se exponen.

Detección, prevención y mitigación

Una vez comprendidos los riesgos a los que están expuestos los NNA en internet, es necesario gestionarlos. Según resume el sitio de IBM, tres pasos son importantes en el proceso de gestión de riesgos: la identificación, la evaluación y la mitigación (IBM, s.f.)[48]

La identificación refiere a la detección temprana de peligros y amenazas lo que nos permite actuar de manera inmediata para la prevención.

Según Cabrera (2020, p.17), la identificación temprana implica monitorear las plataformas donde los NNA interactúan, como redes sociales y foros, para detectar señales de peligro.[49]

Para ello, los algoritmos de inteligencia artificial pueden rastrear patrones de comportamiento relacionados con grooming en línea o detectar CSAM (material de abuso sexual infantil) y generar alertas tempranas para la intervención.

Una vez identificados, se debe analizar los riesgos, teniendo en cuenta factores con relación al uso y comportamiento de los NNA en las plataformas digitales, su condición de vulnerabilidad, el impacto de las consecuencias, etc. Este análisis permitirá hacer una valoración de los riesgos para diseñar estrategias de prevención.

La prevención implica tomar medidas para proteger a los NNA como la difusión de estrategias de protección y recomendaciones para que padres y docentes supervisen el uso de dispositivos conectados a internet como también las campañas educativas que capaciten a los NNA en la identificación de conductas inapropiadas, fomentando el diálogo y la confianza con los adultos de su círculo más cercano.

Las herramientas de control parental también permiten a los responsables de los NNA monitorear en línea el contenido que consumen y supervisar con quién interactúan en el entorno digital, reduciendo la exposición a situaciones de riesgo.

Cuando los riesgos no han podido ser prevenidos y la conducta ilícita ha sido desplegada resulta esencial implementar estrategias de mitigación. La mitigación refiere a las acciones concretas destinadas a reducir el impacto negativo y contener los

[48] IBM. (s.f.). *¿Qué es la gestión de riesgos?* Recuperado de https://www.ibm.com/mx-es/topics/risk-management

[49] Cabrera, L. (2020). *Protección infantil en entornos digitales: Prevención y educación frente a riesgos en internet.* Buenos Aires: Editorial Kapelusz.

daños derivados. En este contexto, la mitigación implica tomar medidas inmediatas que aseguren una respuesta rápida y eficaz, con el fin de minimizar las consecuencias para las víctimas.

La implementación de tecnologías basadas en IA facilita la adopción de medidas inmediatas y eficaces para atenuar los efectos adversos generados por situaciones de riesgo, contribuyendo a la contención y reducción del daño potencial o real en casos de delitos contra la integridad sexual de NNA en entornos digitales.

Una de las medidas más efectivas implementadas a través de la inteligencia artificial es la eliminación automatizada de contenido inapropiado, como imágenes, videos o interacciones sospechosas que se distribuyen en plataformas digitales. Este mecanismo es de particular relevancia en casos de material de abuso sexual infantil (CSAM), donde la pronta identificación y supresión del contenido resulta esencial para prevenir su difusión y minimizar el daño a las víctimas involucradas.

Asimismo, la IA permite bloquear de manera automática los sitios web o cuentas implicadas en actividades delictivas, contribuyendo a interrumpir de forma inmediata la continuidad de acciones ilícitas

En escenarios de grooming, cuando la IA detecta en tiempo real patrones de conversación que sugieren conductas abusivas, puede intervenir de forma inmediata bloqueando la comunicación o alertando a los responsables del menor sobre la situación de peligro.

La inteligencia artificial también tiene la capacidad de generar alertas automáticas dirigidas a las autoridades competentes y a los administradores de la plataforma donde ocurrió el incidente. La colaboración entre empresas, organizaciones y organismos públicos es clave las que deben establecer protocolos coordinados que posibiliten una respuesta rápida y efectiva.

IA, Machine Learning y otras aplicaciones.

Para comprender cómo la IA puede aplicarse en la detección, prevención y mitigación de delitos informáticos contra la integridad sexual de NNA, es esencial analizar esta tecnología innovadora, remitirnos a sus orígenes, evaluar su desarrollo actual y proyección futura.

Nos encontramos atravesando la llamada Cuarta Revolución Industrial caracterizada principalmente por las Tecnologías de la Información y de las Comunicaciones Digitales (TICDs) y la llegada de la IA.

Explican Corvalán y Ciraudo (2021, p.268) que, cuando hablamos de innovación y de nuevas Tecnologías de la Información y de la Comunicación, nos referimos a que asistimos a una época en donde se conjugan tres grandes factores interrelacionados: i) capacidad de almacenamiento; ii) velocidad de procesamiento de los datos y de la información; iii) desarrollo progresivo de múltiples sistemas de inteligencia artificial que reconocen patrones para resolver problemas y alcanzar objetivos.[50]

El inicio de la IA va de la mano con la invención de la computadora digital a mediados del siglo XX, la que ya revelaba su capacidad de procesar información de manera similar al cerebro humano. Fue entonces que los investigadores empezaron a estudiar sus alcances.

Uno de los pioneros fue el matemático británico Alan Turing quien, en su artículo *Computing Machinery and Intelligence* publicado en 1950, sostenía la idea de que una máquina podía imitar los procesos de razonamiento humano y para demostrarlo propuso una prueba que hoy se conoce como *Test de Turing*: una persona, frente a conversaciones en lenguaje natural y sin saber con cuál de los dos está interactuando, debe juzgar si las respuestas provienen de un ser humano o de una computadora. Este experimento evalúa la capacidad de una máquina para exhibir un comportamiento inteligente equivalente o indistinguible al de un ser humano (Turing, 1950, p. 433).[51]

Pero el término "*Artificial Intelligence*" fue acuñado por John McCarthy durante la Conferencia de Dartmouth en la Universidad Dartmouth College, Hanover en 1956, quien años después recibió el Premio Turing comúnmente llamado *"el Premio Nobel de*

[50] Corvalán J. G. y Ciraudo D. (2021). *CIBERCRIMEN II, Capítulo IV: Inteligencia Artificial aplicada al Derecho penal y procesal penal.* Editorial B de F.

[51] Alan Turing (1950) *Computing Machinery and Intelligence.* Mind, Volume LIX, Oxford Academic. Recuperado de https://academic.oup.com/mind/article/LIX/236/433/986238

la informática", por sus importantes contribuciones. El informático y matemático la definiría como "la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas informáticos inteligentes" (John McCarthy, 2007, p.2).[52]

En la década de 1960 se desarrollaron los primeros programas de IA y los sistemas expertos que utilizaban conocimientos preprogramados para resolver problemas complejos, ejemplo de ello es **ELIZA**, creado entre 1964 y 1966 por Joseph Weizenbaum, un programa informático de procesamiento del lenguaje natural que emulaba a un psicoterapeuta y el primer **ChatBot** de la historia (Yúbal, 2017).[53]

Años más tarde Arthur Samuel, quien trabajara para la consultora IBM, desarrolló el **Machine Learning**, el modelo de aprendizaje automático que se utiliza ampliamente en aplicaciones de IA. En 1997, la computadora Deep Blue de IBM, entrenada mediante aprendizaje automático, derrotó al entonces campeón mundial de ajedrez Garry Kasparov.

El científico estadounidense Marvin Lee Minsky, reconocido como uno de los pioneros de la inteligencia artificial, cofundó en 2003 el Laboratorio de Inteligencia Artificial del Instituto de Tecnología de Massachusetts (MIT) y contribuyó al desarrollo del razonamiento simbólico, un componente central de la IA.

En 2006, Geoffrey Hinton presentó por primera vez el concepto de **Deep Learning** o aprendizaje profundo para explicar nuevas arquitecturas de redes neuronales que luego desarrollará con Google.

Tiempo después, en 2009, Microsoft se asoció con Dartmouth College para desarrollar **PhotoDNA**. A partir de una base de datos de imágenes y archivos de vídeo conocidos, crea hashes únicos para representar cada imagen, que luego pueden usarse para identificar otras instancias de esas imágenes. Como se verá más adelante, se trata de una tecnología que ayuda a detectar imágenes conocidas de CSAM (Microsoft, 2009).[54]

---

[52] John McCarthy. (2007). *WHAT IS ARTIFICIAL INTELLIGENCE?.* Stanford University.
[53] Yúbal Fernández. (2007). *Así era ELIZA, el primer bot conversacional de la historia.* Xataka. Yúbal Fernández. (2007). *Así era ELIZA, el primer bot conversacional de la historia.* Xataka. Recuperado de https://www.xataka.com/historia-tecnologica/asi-era-eliza-el-primer-bot-conversacional-de-la-historia
[54] Microsoft (2009). *PhotoDNA* Recuperado de https://www.microsoft.com/en-us/photodna

En 2012 Google comienza a desarrollar clasificadores de aprendizaje automático que luego mejorará con la tecnología de redes neuronales profundas (RNPs) para detectar patrones imágenes y vídeos.

Años más tarde, Facebook desarrolla **DeepFace**, un sistema de reconocimiento facial de a través de redes neuronales. Facebook ya utilizaba esta tecnología, aunque menos desarrollada, para sugerir etiquetas en fotografías subidas por los usuarios a la red social. “DeepFace crea modelos 3D de los rostros en fotografías y después los analiza por medio de tecnología de inteligencia artificial conocida como aprendizaje profundo” (O’ Toole, 21 de abril de 2014, CNN en español).[55]

Luego, **Clearview AI** se posicionará como líder en el mercado de esta tecnología.

En 2017, OpenAI, la empresa fundada por Elon Musk y otros, siendo su principal accionista Microsoft, lanzó **GPT-1** cuyas siglas corresponden a Generative Pre-Training, la primera versión del modelo de lenguaje generativo pre entrenado, que luego fue mejorando sus versiones hasta llegar a GPT 4.0. En 2023 la misma compañía diseñó **Sora**, un modelo de conversión de texto a video. A partir de prompt puede generar escenas de video como si fueran reales. Se denomina "prompt" a las instrucciones, órdenes o premisas ingresadas para que GPT o Sora lleven a cabo la acción.

Pero entonces ¿Que es la Inteligencia Artificial? Retomando el concepto de McCarthy, diremos que IA es el campo de la ciencia de la informática, que se ocupa del desarrollo de los sistemas capaces de gestionar la información, aprender de los datos y en base a estos dar respuestas o soluciones.

IBM explica en su sitio web que, un sistema de IA es esencialmente un sistema informático que utiliza algoritmos de IA para lograr objetivos específicos con un cierto grado de autonomía. Por sistema entendemos la combinación de software y hardware diseñados para producir resultados basados en los insumos que reciben. Un algoritmo puede ser definido como un conjunto preciso de instrucciones o reglas o como una

[55] James O’ Toole. (21 de abril de 2014). *¿Cómo funciona el reconocimiento facial de Facebook?* CNN en español. Recuperado de https://cnnespanol.cnn.com/2014/04/21/como-funciona-el-reconocimiento-facial-de-facebook

serie metódica de pasos que pueden utilizarse para hacer cálculos, resolver problemas y tomar decisiones.[56]

Como hemos visto, a lo largo de la historia, la IA ha evolucionado incluso actualmente se encuentra en desarrollo. No existe un criterio unánime para clasificar la IA, aunque todos hacen referencia a sus diferentes etapas o fases de evolución. A continuación, se exponen los criterios de algunos autores:

Schneppat (2019) explica que, según el grado de desarrollo, podemos hablar de tres niveles de IA:

- **ANI** (por sus siglas en inglés de Artificial Narrow Intelligence): también conocida como IA estrecha o débil. Son sistemas diseñados para realizar tareas específicas y no tienen capacidad de aprendizaje o adaptación por sí mismos, requieren ser programados y entrenados. Para programarlos se utiliza algoritmos y reglas que aplican el razonamiento lógico y se entrenan suministrándole información, datos. Sólo pueden tomar decisiones o realizar acciones basadas en dicha información y para lo cual fue programado. La IA que nos rodea hoy (smartphones, en el reconocimiento de voz, la identificación de imágenes o la traducción de idiomas, al igual que GPS o el buscador de Google) es IA débil. ANI puede igualar o superar a la inteligencia y eficiencia humana solo en el área específica en la que opera.

- **AGI** (Artificial General Intelligence o Inteligencia Artificial General): se alcanza cuando una máquina adquiere capacidades cognitivas a nivel humano. Hablamos de un sistema capaz de razonar y resolver problemas, adaptarse a nuevas situaciones, comprender conceptos abstractos, aprender y mejorar. Si bien los sistemas ANI también son capaces de aprender de los datos y mejorar, AGI puede ampliar su conocimiento a nuevas situaciones y funciones para las que no ha sido entrenada. Esto significa que podría potencialmente aprender nuevas

[56] IBM. (s.f.). *What is artificial intelligence (IA)?* Recuperado de https://www.ibm.com/es-es/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=inteligencia%20artificial

habilidades y generara nuevos conocimientos sin previa programación, lo que conduciría a avances sin precedentes en la IA. Sin embargo, a medida que se vuelve más capaz de aprender y modificar su propio funcionamiento, puede resultar impredecible. Por ello, el desarrollo de AGI requiere un marco ético y normativo y una consideración cuidadosa de los riesgos potenciales asociados con la tecnología. Algunos sostienen que estamos al borde de lograr este nivel de desarrollo de IA, lo cierto es que hoy se trata de un concepto teórico.

- **ASI** (Artificial Superintelligence): se trata de un nivel hipotético de IA que aún no ha sido desarrollado, que tendría el potencial de replicar la inteligencia humana no solo en habilidades de razonamiento matemático y lógico, sino también en creatividad, subjetividad, experiencias, comprender el lenguaje natural incluso superar ampliamente las capacidades cognitivas de los seres humanos. (Schneppat, 2019).[57]

Arendt Hintze, profesor de Biología Integrada y Ciencias de la Computación de la Universidad de Michigan propone una clasificación basada en la capacidad predictiva y en los niveles de complejidad, distinguiendo entre:

- **Máquinas reactivas:** es el nivel más simple e incluye todos aquellos sistemas que, si bien hacen uso de la inteligencia artificial, no son capaces de recordar ni de usar experiencias previas para tomar decisiones. Estos modelos que utilizan automatización suelen ser menos complejos y sofisticados desde el punto de vista de la programación.
- **Memoria limitada:** a diferencia de las máquinas reactivas, sí cuentan con memoria, aunque limitada que les permite generar aprendizajes a partir de los datos. Esto hace que sea posible que tomen decisiones en base a la experiencia.
- **Teoría de la mente:** en esta categoría hipotética, los sistemas son capaces de procesar emociones y realizar procesos de reflexión propios de la mente humana.

[57] Schneppat Jörg-Owe (2019). *Types of AI*. Schneppat AI. Recuperado de https://schneppat.com/types-of-ai.html

- **Autoconciencia:** se trata del nivel más alto que puede desarrollar la inteligencia artificial y supone que las máquinas sean capaces no sólo de comprender emociones, sino también de tener propias. Al igual que la teoría de la mente, se trata de un nivel hipotético, y no hay precedentes a la fecha. (Hintze, s.f.). [58]

Otra clasificación propuesta es en base al tipo de aprendizaje y distingue entre el aprendizaje automático o machine learning, el aprendizaje profundo o deep learning y el sistema experto. Analicemos cada una:

- **Aprendizaje automático o Machine Learning:** a través de algoritmos, el sistema analiza los datos y aprende de ellos. Se trata de un subcampo de la IA que aprende automáticamente de la información suministrada, detectan patrones relevantes y sobre estos incluso, pueden tomar una decisión o elaborar una predicción a través de dos métodos fundamentalmente: supervisado (los algoritmos tienen una serie de variables objetivo, con unos valores específicos que se utilizan para entrenar al modelo) y el no supervisado (la máquina aprende y clasifica las variables de forma automática para realizar sus predicciones). Aunque el aprendizaje automático domina hoy en día el campo de la IA, tiene sus limitaciones ya que requiere tiempo para alimentar las bases de datos y las abstracciones que permiten al sistema aprender (IBM, s.f.).[59]

- **Aprendizaje profundo o Deep Learning:** se trata de un sistema mucho más complejo basado en redes neuronales artificiales. Una red neuronal es una red de entidades interconectadas conocidas como nodos en la que cada nodo es responsable de un cálculo simple. Las redes neuronales están compuestas por capas de nodos, distribuidas en: una capa de entrada, una o más capas ocultas y una capa de salida. Cada capa contiene una o varias neuronas. Existen varios

[58] Arend Hintze. (s.f.). *Tipos de inteligencia artificial.* Tableau. Recuperado de https://www.tableau.com/es-mx/data-insights/ai/tipos-de-inteligencia-artificial

[59] IBM. (s.f.). *What is machine learning?* Recuperado de https://www.ibm.com/topics/machine-learning#:~:text=Machine%20learning%20(ML)%20is%20a,learn%2C%20gradually%20improving%20its%20accuracy.

tipos de redes neuronales que se utilizan para diferentes casos y tipos de datos (IBM, s.f.).[60]

En lugar de la lógica lineal, refiere Banafa (2022), el aprendizaje profundo se basa en las teorías sobre el funcionamiento del cerebro humano por lo que el programa, formado por capas intrincadas de nodos interconectados, aprende reordenando las conexiones entre los nodos tras cada nueva experiencia.[61]

Por ello decimos que funciona de manera similar a las neuronas del cerebro humano, ya que se establecen conexiones entre nodos, se manda información y se sacan conclusiones a partir de los datos introducidos inicialmente. Una red neuronal es entrenada o alimentada en base a grandes cantidades de datos y reglas sobre las relaciones entre estos y a través de un programa se le puede indicar al sistema cómo comportarse en respuesta a un estímulo externo o la propia red puede iniciar la actividad por sí misma, dentro de los límites de su acceso al mundo externo. (Schneppat, 2019).[62]

- **Sistema experto:** es un programa informático diseñado para resolver problemas específicos mediante la aplicación de un conjunto de reglas predefinidas en un área particular. Estos sistemas funcionan sobre una base de conocimientos extensa y detallada, junto con un motor de inferencia que aplica esas reglas para llegar a conclusiones o recomendaciones. Se utilizan principalmente en campos como las finanzas, la ingeniería, y la medicina. Ayudan en la toma de decisiones complejas que normalmente serían realizadas por profesionales altamente capacitados. Un ejemplo son los sistemas de diagnóstico de enfermedades, que analizan síntomas y datos clínicos para sugerir posibles diagnósticos o tratamientos, facilitando el trabajo de médicos.[63]

Redes Neuronales Convolucionales

---

[60] IBM. (s.f.). *What is deep learning?* Recuperado de https://www.ibm.com/es-es/topics/deep-learning
[61] Banafa Ahmed (14 de octubre 2022). *Intellectual Abilities of Artificial Intelligence.* Spark BBVA. Recuperado de https://www.bbvaspark.com/contenido/en/news/intellectual-abilities-of-artificial-intelligence/
[62] Schneppat Jörg-Owe (2019). *Types of AI*. Schneppat AI. Recuperado de https://schneppat.com/types-of-ai.html
[63] Arend Hintze. (s.f.). *Tipos de inteligencia artificial.* Tableau. Recuperado de https://www.tableau.com/es-mx/data-insights/ai/tipos-de-inteligencia-artificial

Dentro del aprendizaje profundo o deep learning, encontramos a las redes neuronales convolucionales (ConvNets o CNN) las que se utilizan generalmente para tareas de clasificación y computer vision. Antes de las CNN, la extracción de características se hacía con métodos manuales por lo que requería mucho tiempo para identificar objetos en imágenes.

Las redes neuronales convolucionales se distinguen de otras redes neuronales por su rendimiento superior con entradas de imagen, voz o señales de audio. Tal como explica la consultora IBM en su sitio web, proporcionan un enfoque más escalable para las tareas de clasificación de imágenes y reconocimiento de objetos al aprovechar los principios del álgebra lineal, en concreto la multiplicación de matrices, para identificar patrones en una imagen. Estas redes pueden exigir un uso intensivo de recursos informáticos y requerir unidades de procesamiento gráfico (GPU) para entrenar los modelos (IBM, s.f.).[64]

Las redes neuronales convolucionales se componen de tres tipos principales de capas, según expone IBM en su sitio web:

1. Capa convolucional
2. Capa de agrupación
3. Capa totalmente conectada

La capa convolucional es la primera, pueden seguirle otras capas convolucionales luego la capa de agrupación y la capa final es la capa totalmente conectada. Con cada capa, la CNN aumenta en complejidad: las primeras capas se centran en características simples, como colores y bordes. A medida que los datos de la imagen avanzan a través de las capas, la CNN comienza a reconocer elementos o formas más grandes hasta que finalmente identifica el objeto esperado (IBM, s.f.).[65]

Aprendizaje automático vs. redes neuronales artificiales

[64] IBM. (s.f.). *What are convolutional neural networks?* Recuperado de https://www.ibm.com/es-es/topics/convolutional-neural-networks
[65] IBM. (s.f.). *What are convolutional neural networks?* Recuperado de https://www.ibm.com/es-es/topics/convolutional-neural-networks

Pese a que ambos son modelos de IA, el aprendizaje automático y la red neuronal se diferencian en varios aspectos.

Un modelo de aprendizaje automático se nutre de grandes volúmenes de datos, extrayendo patrones y regularidades para, a partir de estos, tomar decisiones o realizar predicciones. A medida que el modelo recibe nuevos datos, ajusta su comportamiento en función de la información previamente aprendida, lo que le permite adaptarse a diferentes situaciones. Aunque estos modelos son altamente flexibles y capaces de evolucionar con cada nuevo conjunto de datos, su capacidad de aprendizaje depende exclusivamente de los patrones e información que se le suministren, ya que estos constituyen su única fuente de entrada.

En contraste, las redes neuronales artificiales, inspiradas en la estructura del cerebro humano, presentan una arquitectura más compleja. Estas redes constan de múltiples capas de nodos o 'neuronas', organizados en capas de entrada, ocultas y de salida. Cada nodo en una capa recibe los datos de la capa anterior, los procesa y luego envía los resultados a la siguiente capa. Este proceso de propagación de la información a través de varias capas permite que las redes neuronales realicen tareas más sofisticadas, como la clasificación de imágenes, el procesamiento de lenguaje natural o el reconocimiento de patrones complejos. La capacidad de cada nodo para ajustar los procesos a la información que recibe permite a la red mejorar su precisión a lo largo del tiempo, haciendo que sea una herramienta poderosa en contextos donde los datos son multidimensionales o altamente complejos.

Cuantas más capas y más neuronas artificiales tiene un sistema, mejor procesa la información ya que las capas anidadas dentro pasan los datos a través de los nodos y organiza los algoritmos de tal manera que puede tomar decisiones precisas por sí misma. Es decir, no requiere la intervención humana incluso son capaces de aprender a través de sus propios errores (IBM, s.f.).[66]

Entre los aportes más comunes que trajo la IA y que hoy forman parte de nuestra vida, podemos mencionar:

[66] IBM. (s.f.). *Deep learning versus machine learning.* Recuperado de https://www.ibm.com/topics/artificial-intelligence

- ✔ Reconocimiento automático del habla (ASR): es una función que tienen la mayoría de los dispositivos móviles como Siri de iPhone o Speech-to-Text de Google. Utiliza el procesamiento del lenguaje natural (NLP) para convertir el habla en formato escrito o realizar búsquedas de voz. Incluso hoy existe Voice Match, una tecnología para ayudarle al asistente de Google a reconocer la voz y verificar la identidad antes de brindar resultados personales (Google, s.f.). [67]
- ✔ Chatbots: es un programa informático que utiliza inteligencia artificial (IA) y procesamiento del lenguaje natural (NLP) para comprender las preguntas de los clientes y automatizar las respuestas a dichas preguntas, simulando la conversación humana. A través de esta tecnología Las empresas pueden responden preguntas frecuentes generalmente en sitios de comercio electrónico o de servicios, personalizar las experiencias de los clientes, el e-commerce etc (IBM, s.f.).[68]
- ✔ Motores de recomendaciones: utilizando datos de comportamiento de consumo anteriores, los algoritmos de IA permiten descubrir tendencias de datos que pueden utilizarse para desarrollar estrategias de venta, incluso Netflix para ofrecer contenido de preferencia.
- ✔ Visión por ordenador: basada en redes neuronales convolucionales, tiene aplicaciones en el etiquetado de fotografías en redes sociales.
- ✔ Chat GPT: como vimos se trata de una aplicación de inteligencia artificial desarrollado en 2022 por OpenAI que interactúa de forma conversacional. El formato de diálogo hace posible que ChatGPT responda preguntas y está capacitado para seguir una instrucción en un mensaje y proporcionar una respuesta detallada.

El uso de la IA para detectar, prevenir y mitigar los delitos informáticos contra la integridad sexual de NNA.

[67] Google (s.f.). *Voice Match.* Recuperado de https://support.google.com/chromecast/answer/9071681?hl=es&co=GENIE.Platform%3DAndroid

[68] IBM. (s.f.). *What is a chatbot?* Recuperado de https://www.ibm.com/topics/chatbots#:~:text=A%20chatbot%20is%20a%20computer,conversation%20with%20an%20end%20user.

Como ya se ha mencionado antes, la identificación de pedófilos en entornos digitales no es trabajo sencillo, debido al anonimato que caracteriza a internet y a las sofisticadas técnicas que emplean los delincuentes para evadir la detección y ocultar su rastro, como la creación de perfiles falsos, el uso de programas destinados a interferir en la trazabilidad de las direcciones IP, el uso de IP dinámicas, el acceso a redes públicas no seguras o la utilización de la darknet.

Sumado a ello, la masividad de usuarios conectados a internet y el volumen de datos e información que comparten a cada segundo, hace que la tarea de monitorear y controlar sea extremadamente compleja. Ante la imposibilidad humana de revisar la información que se comparte y detectar CSAM (child sexual abuse material) resulta necesario recurrir a tecnologías avanzadas y mecanismos de vigilancia automatizados que complementen el trabajo humano para garantizar entornos más seguros.

En este sentido, la IA se presenta como una opción eficiente para realizar este trabajo ya que es capaz de procesar grandes cantidades de información de manera rápida y precisa, reduciendo significativamente los tiempos y costos. Al automatizar este proceso, el capital humano puede enfocarse en tareas más especializadas, como la investigación y el seguimiento de casos, optimizando los recursos disponibles.

La IA es una herramienta que podemos poner al servicio ya que, sin ella, no sería posible la protección en tiempo real, a escala, ni la localización de patrones en base a tendencias a largo plazo, debido al volumen de datos que se generan en línea todos los días (GEGENHEIMER et al, 2019, p.27).[69]

Los algoritmos de IA tienen además la capacidad de identificar características, correlaciones y patrones que podrían pasar desapercibidos para el ojo humano lo que permite reducir los errores manuales y eliminar los sesgos cognitivos, es decir, las interpretaciones subjetivas o juicios erróneos que pueden surgir del razonamiento humano. Otro beneficio es que la IA no está sujeta a las mismas limitaciones que las personas, lo que le permite trabajar de manera continua, sin interrupciones ni restricciones de tiempo. Esto garantiza una vigilancia constante y eficiente, maximizando la capacidad de respuesta frente a amenazas digitales.

[69] GEGENHEIMER Scott et al (2019). *Seguridad de los niños en línea: minimizando el riesgo de la violencia, el abuso y la explotación en línea.* UNESCO.

El análisis automatizado de contenidos digitales compartidos en línea permite, mediante algoritmos de reconocimiento de imágenes, detectar CSAM. Como ya se dijo antes, la pronta identificación y supresión del contenido resulta esencial para prevenir su difusión y minimizar el daño a las víctimas involucradas.

Automatizar este proceso, no solo facilita la identificación rápida de contenidos ilegales contribuyendo a detener su difusión, también facilita la identificación de los sitios webs y las cuentas implicadas en estas actividades delictivas. Una vez identificadas se puede notificar a los proveedores de hosting/servidores o a los responsables de las plataformas, según sea el caso, para bloquear dichas cuentas o sitios y poner en conocimiento a las autoridades para que intervengan rápidamente y puedan establecer y juzgar a los autores.

Además, las plataformas de aprendizaje automático permiten desarrollar modelos y algoritmos adaptados a las necesidades específicas del contexto. Esto habilita la creación de criterios de búsqueda más precisos, ajustados a la naturaleza de los delitos o patrones de conducta a investigar. De esta forma, los resultados obtenidos responden a patrones que coinciden con lo solicitado, incrementando la eficiencia en la identificación de material ilegal.

Con relación a la investigación, la IA posibilita que las autoridades y organismos responsables puedan acceder a grandes bases de datos con velocidad y precisión. Con la información obtenida, se puede generar estadísticas y mediante las herramientas de análisis predictivo, vaticinar tendencias y resultados futuros lo que permite diseñar políticas de seguridad y prevención.

La IA también puede aplicarse para la prevención del grooming, contribuyendo a la creación de entornos en línea más seguros para NNA. ¿Cómo lo logra? Al monitorear redes sociales y plataformas digitales, la IA puede identificar patrones de comportamiento asociados con el ciberacoso mediante algoritmos de procesamiento de lenguaje natural (PNL) en el análisis de texto. Esto le permite detectar palabras, frases o expresiones ofensivas, amenazantes o denigrantes en conversaciones, publicaciones o mensajes.

Cabe aclarar, que la IA tiene ciertas limitaciones, como la dificultad para interpretar correctamente el contexto o la intención detrás de un mensaje. Esto puede generar falsos positivos o negativos en la detección de ciberacoso, todo dependerá de cuán entrenado esté el modelo y de los algoritmos utilizados.

Para obtener resultados más precisos, muchas plataformas están invirtiendo en el desarrollo de modelos más avanzados de IA que integren una mayor capacidad de análisis contextual. Las empresas tecnológicas, en su responsabilidad de controlar el contenido compartido por los usuarios a sus plataformas, podrían implementar herramientas de IA que analicen automáticamente emitiendo alertas inmediatas cuando se detecta material sospechoso. Estas herramientas permiten intervenir antes de que un NNA esté expuesto a situaciones de grooming o ciberacoso, contribuyendo así a un entorno digital más seguro.

Asimismo, la IA puede complementar el uso de herramientas de control parental, que juegan un rol clave en la protección de los NNA en internet. permiten a padres y tutores supervisar la actividad en línea de los menores, configurando filtros de contenido y monitoreando o restringiendo el acceso a determinadas aplicaciones o sitios web.

La incorporación de IA en estas herramientas optimiza la precisión en la detección de comportamientos de riesgo, lo que facilita la emisión de alertas en tiempo real ante posibles interacciones peligrosas. De este modo, la IA no solo refuerza las capacidades preventivas de las plataformas, sino que también se convierte en una herramienta de apoyo para los tutores, ayudándolos a intervenir de manera proactiva en la protección de sus hijos.

Precedentes y nuevas aplicaciones de la IA para la prevención y detección temprana de delitos de abuso sexual de NNA en plataformas digitales.

En agosto de 2014, un hombre de 41 años fue detenido en Houston Texas, acusado de utilizar su cuenta de correo Gmail para enviar imágenes de menores desnudos. Se trataba de un pedófilo reincidente y fue Google quien alertó a las autoridades, según publicó la cadena de noticias BBC Mundo en sus portales de internet (BBC Mundo, 2014).[70]

La noticia tomó repercusión no sólo por tratarse de un hecho de abuso a menores, sino que además dejó interrogantes acerca de la privacidad de los correos electrónicos y sobre la vigilancia de Google en internet. La compañía se pronunció en aquel entonces explicando que no vulneraba la privacidad de sus usuarios ni revisaba las cuentas, sino que disponía de una tecnología que le permitía escanear automáticamente toda la información a fin de detectar contenido ilegal. En caso de advertir alguna sospecha con relación a material de abuso sexual de NNA, inmediatamente alertaba al NCMEC (National Center for Missing & Exploited Children) quien notificaba a las autoridades. Estas, basándose en el indicio que Google aporta se encargaban de corroborarlo (BBC Mundo, 2014).[71]

El NCMEC es un organismo que, gracias a la ayuda de grandes compañías tecnológicas (como Google, Microsoft y Facebook) ha elaborado una gran base de datos de material de abuso sexual infantil (child sexual abuse material - CSAM), para que luego se puedan hacer comprobaciones automáticas. Esta a su vez, alimenta la base de datos ICSE de la Unidad de Delitos contra menores de Interpol, a la cual tienen acceso los especialistas en identificación de víctimas a través del sistema mundial de comunicación policial de INTERPOL (I-24/7), que también utiliza esta tecnología para la detección y comparación de imágenes, según explica dicha Organización (Interpol, 2019).[72]

Chamorro Concha explica que a la base de datos contribuyen 53 países miembros alimentándola con material resultante de allanamientos o actividades de monitoreo.

---

[70] BBC Mundo (5 de agosto de 2014) *Por qué Google está revisando los correos de Gmail.* Recuperado de https://www.bbc.com/mundo/noticias/2014/08/140805_google_pornografia_gmail_am

[71] BBC Mundo (5 de agosto de 2014) *Por qué Google está revisando los correos de Gmail.* Recuperado de https://www.bbc.com/mundo/noticias/2014/08/140805_google_pornografia_gmail_am

[72] Interpol (8 de noviembre de 2019). *La base de datos de INTERPOL permite identificar a menores víctimas de delitos sexuales.* Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/La-base-de-datos-de-INTERPOL-permite-identificar-a-menores-victimas-de-delitos-sexuales

Estas imágenes y videos se comparan y permite que los investigadores especializados intercambien datos para tratar de establecer interconexiones entre las víctimas, los abusadores y el lugar dónde se encuentran tanto las víctimas como los agresores. Pero sólo seis países de América Latina se encuentran conectados a ICSE: Argentina, Brasil, Chile, Colombia, El Salvador y Guatemala (Chamorro Concha, 2021, p. 263).[73]

En su momento, Google además manifestó que dentro de las políticas de seguridad y en los términos de uso que generalmente los usuarios aceptan sin leer, hay una sección que se titula "Política sobre seguridad infantil " donde se advierte:

> Sexualización de menores: no se permite el contenido sexual explícito en el que se muestre a menores o en el que se los explote sexualmente, lo que incluye publicar material con fines humorísticos donde aparezcan menores desnudos. Denunciamos el contenido que incluye imágenes de abuso sexual infantil al National Center for Missing & Exploited Children, que colabora con organismos públicos de todo el mundo encargados de velar por el cumplimiento de las leyes Eliminación del contenido: si creemos razonablemente que parte de su contenido infringe estas condiciones o las condiciones o las políticas adicionales específicas de los servicios, viola la legislación aplicable o podría dañar a nuestros usuarios, a terceros o a Google, nos reservamos el derecho de eliminar ese contenido de forma parcial o total conforme a la legislación aplicable. Algunos ejemplos son la pornografía infantil (Google, s.f.).[74]

¿Y de qué se trataba la tecnología a la que hacía referencia Google? Se trataba de función hash. Susan Jasper, vicepresidenta de Operaciones de Confianza y Seguridad explica en el Blog de Google, cómo se utiliza la coincidencia de hash para identificar

[73] Chamorro Concha, Gabriela (2021). CIBERCRIMEN II, Derecho procesal Penal. *Material de explotación sexual infantil y la importancia de las investigaciones en redes.* BdeF Editorial
[74] Google (s.f.). Política sobre seguridad infantil. Recuperado de https://support.google.com/youtube/answer/2801999?hl=es

material de abuso sexual infantil conocido, indicando que esta tecnología asigna a las imágenes y vídeos una firma digital única ("hash") y la compara con la base de datos de otras firmas ("hashes") que se obtiene de diversas fuentes como Internet Watch Foundation (IWF) y National Center for Missing and Exploited Children (NCMEC). Una vez comparadas, si advierte coincidencia denuncian a las autoridades. (Susan Jasper, 2022).[75]

Sin embargo, esta tecnología tiene una limitación: con tan sólo modificar las imágenes (como cambiar los colores, el brillo o editar algún elemento de la fotografía) ya no podrían ser identificadas.

PhotoDNA de Microsoft

PhotoDNA desarrollada por Microsoft ayuda a resolver este problema. Se trata de “una tecnología capaz de detectar automáticamente cualquier contenido abusivo de menores, independientemente de que se haya alterado la imagen” asegura Richard Boscovich, Asesor General de Digital Crimes Unit de Microsoft en una entrevista del diario El Mundo (Boscovich, 2016).[76]

Boscovich explica que, para ello convierte las imágenes originales (las que se encuentran registradas por el NCMEC (National Center for Missing and Exploited Children) a un formato en escala de grises, luego se la divide en celdas, se registran los metadatos y relaciones entre los elementos (como la distancia entre ojos) para, finalmente, asignarles un valor numérico individual y completamente anónimo que representa los rasgos únicos de cada zona. Una vez realizado todo este proceso, 'tan sólo' hay que rastrear y comparar cada una de las secciones con toda la base de datos y los contenidos que se están distribuyendo en tiempo real en Internet (Boscovich, 2016).[77]

---

[75] Susan Jasper (2022). *Cómo detectamos, eliminamos y denunciamos el material de abuso sexual infantil.* Recuperado de https://blog.google/intl/es-es/productos/informacion/2022_10_como-detectamos-eliminamos-y/

[76] Boscovich R. (7 sept 2016) PhotoDNA: *Así es la herramienta que atrapa a los pederastas en Internet.* Recuperado de https://www.elmundo.es/economia/2016/09/07/57cd61f946163f30748b45d7.html

[77] Boscovich R. (7 sept 2016) PhotoDNA: *Así es la herramienta que atrapa a los pederastas en Internet.* Recuperado de https://www.elmundo.es/economia/2016/09/07/57cd61f946163f30748b45d7.html

De lo indicado por el especialista se desprende que el proceso es el siguiente:

1 PhotoDNA convierte la imagen original a un formato en escala de grises, modificando también el tamaño hasta que coincida con el establecido.
2 Luego divide la imagen (con tamaño modificado y en escala de grises) en cuadrados más pequeños o celdas.
3 Para cada cuadrado o celdas calcula distintos parámetros, como la variación del tono de negro de cada píxel, las relaciones entre los elementos (distancia entre ojos, etc.) y se registran los metadatos.
4 A posterior se le asigna un valor numérico individual y completamente anónimo que representa los rasgos únicos de cada zona.
5 Con todos los valores de cada cuadrado o celdas se crea un histograma. Estos valores numéricos, finalmente, se convierten en la firma única o hash que se asigna a cada imagen.

En conclusión, las firmas generadas por PhotoDNA obtenidas a partir de la información de la base de datos del NCMEC, junto con las firmas específicas creadas por otros algoritmos "hashing", permite cotejar las imágenes de sus archivos en busca de posibles coincidencias.

Richard Boscovich, en dicha entrevista, aseguró que no se trataba de un software de reconocimiento facial y que no puede utilizarse para identificar a una persona u objeto en una imagen, como tampoco es reversible un hash de esta herramienta, por lo tanto, no se puede utilizar para recrear una imagen (Boscovich, 2016).[78]

La compañía **Microsoft** ha donado PhotoDNA al Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) con el fin de ayudar a combatir la explotación infantil. También ha puesto a disposición esta herramienta a aquellas compañías, organizaciones no gubernamentales que quieran sumarse a la lucha contra la pornografía infantil y de este modo puedan detectar imágenes ilegales en sus servicios online. Pese a ser competidores directos de Microsoft, Facebook, Twitter y Google también utilizan esta tecnología con el mismo propósito.

[78] Boscovich R. (7 sept 2016) PhotoDNA: *Así es la herramienta que atrapa a los pederastas en Internet.* Recuperado de https://www.elmundo.es/economia/2016/09/07/57cd61f946163f30748b45d7.html

La contribución de la tecnología PhotoDNA por parte de Microsoft es otro ejemplo de cómo la cooperación entre el sector público y el privado puede generar un valor adicional, que en este caso servirá para salvar a niños víctimas de abusos sexuales. INTERPOL continuará colaborando con sus aliados para luchar contra este tipo de crímenes, los cuales están en constante evolución, afirmó Glyn Lewis, Director de Delincuencia Especializada y Análisis de INTERPOL (Lewis, 2015). [79]

"Es esencial que todo el material sobre explotación y abuso de menores se analice de manera tan minuciosa y eficaz como sea posible, a fin de ayudar a identificar y rescatar a las víctimas cuanto antes", señaló Mick Moran, Subdirector de Trata de Personas y Explotación Infantil de INTERPOL y añadió "Asimismo es esencial evitar la duplicación de esfuerzos para que los funcionarios no empleen su precioso tiempo en tratar de identificar a una víctima que ya puede haber sido rescatada. La integración de PhotoDNA en la base de datos ICSE ayudará a nuestros países miembros a resolver estos problemas" (Moran, 2015).[80]

PhotoDNA sin duda es una herramienta de indiscutible utilidad, pero no parece ser la solución definitiva ya que, si bien reconoce imágenes que puedan haber sido modificadas, sólo sirve para detectar aquellas imágenes previamente identificadas que se encuentran en la base de datos del NCMEC. Entonces ¿cómo es posible identificar nuevo CSAM?

Tal como indica Child Rights International Network, la detección de nuevo CSAM plantea mayores desafíos técnicos que la detección de imágenes conocidas ya que no se puede lograr mediante el "hashing". La identificación de CSAM desconocido sólo puede realizarse mediante IA, basada en el aprendizaje automático. Los clasificadores (algoritmos que clasifican datos en clases basándose en el reconocimiento de patrones) se pueden entrenar para detectar desnudez, rostros, colores, etc. Es

---

[79]Lewis Glyn (14 de abril de 2015) *La tecnología de Microsoft impulsa la labor mundial de identificación -a través de INTERPOL- de niños víctimas de abusos.* INTERPOL. Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2015/La-tecnologia-de-Microsoft-impulsa-la-labor-mundial-de-identificacion-a-traves-de-INTERPOL-de-ninos-victimas-de-abusos.

[80] Moran Mick (14 de abril de 2015) *La tecnología de Microsoft impulsa la labor mundial de identificación -a través de INTERPOL- de niños víctimas de abusos.* Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2015/La-tecnologia-de-Microsoft-impulsa-la-labor-mundial-de-identificacion-a-traves-de-INTERPOL-de-ninos-victimas-de-abusos

complejo detectar la edad de una persona que se muestra en el contenido, sobre todo si se trata de un adolescente o un adulto joven (Rights, 2023). [81]

Los sistemas de aprendizaje automático procesan los datos proporcionados y aprenden de ellos de manera continua. Cuanta mayor cantidad de datos tienen para analizar, más precisos y efectivos se vuelven en la toma de decisiones. Solo un sistema de IA es capaz de procesar grandes volúmenes de información a alta velocidad y automatizar esta tarea.

Sin embargo, el entrenamiento de estos sistemas para reconocer CSAM requiere la utilización de grandes volúmenes de imágenes y videos relacionados con este tipo de contenido, con el fin de que el modelo pueda identificar patrones y características específicas.

Este proceso genera un debate sobre las implicaciones legales y éticas, ya que involucra la manipulación de material sensible y potencialmente ilegal. Por ello, es fundamental establecer protocolos rigurosos que aseguren la protección de los datos y el cumplimiento estricto de las normativas legales mientras se desarrollan soluciones tecnológicas para combatir estos delitos.

API Content Safety de Google

A la pregunta de cómo detectan material de abuso sexual de NNA, Susan Jasper Vicepresidenta de Operaciones de Confianza y Seguridad de la compañía, explica que la compañía utiliza dos tecnologías igualmente importantes para identificar de forma proactiva material de abuso sexual infantil: la coincidencia de hash y la IA. (Jasper Susan, 2022). [82]

Para identificar CSAM conocido se sirve de la tecnología de coincidencia de hash mientras que para CSAM desconocido, con la ayuda de la IA, Google desarrolló la API Content Safety. Gracias al aprendizaje automático, API Content Safety puede reconocer

[81] Child Rights International Network (2023). *Explicando la tecnología para detectar abuso sexual infantil online.* Recuperado de https://home.crin.org/readlistenwatch/stories/explainer-detection-technologies-child-sexual-abuse-online

[82] Jasper Susan (2022). *Cómo detectamos, eliminamos y denunciamos el material de abuso sexual infantil.* Recuperado de https://blog.google/intl/es-es/productos/informacion/2022_10_como-detectamos-eliminamos-y/

de forma proactiva, con más rapidez y precisión nuevo CSAM en el procesamiento de imágenes ya que logra identificar y extraer características claves de estas y utilizarlas como entrada para un modelo de Machine Learning (Google, s.f.). [83]

Pero ¿Cómo funciona esta tecnología? Básicamente en tres pasos:

1. Datos de entrenamiento: las imágenes CSAM de la base de datos del NCMEC serían los datos de entrenamiento que se dispone.
2. Extracción de características: mediante algoritmos de extracción de características se selecciona las aquellas relevantes de cada imagen.
3. Creación de un modelo de Machine Learning: estas características se agregan a un modelo de Machine Learning, que las dividirá en sus distintas categorías y luego utilizará esta información durante el análisis y la clasificación de nuevos objetos (Mathworks s.f.).[84]

Si bien la herramienta está basada en aprendizaje automatizado, resulta necesario verificar si se ha identificado con precisión el material de abuso sexual infantil (CSAM) lo que requiere supervisión humana, es decir puede tener un porcentaje de "falsos positivos" o "tasa de error". Pero el gigante tecnológico asegura que se encuentra trabajando en redes neuronales profundas para el procesamiento de imágenes, lo que le permitirá detectar incluso sin supervisión humana.

CSAI Match por YouTube

Se trata de una API que ayuda a identificar vídeos que se han vuelto a subir, previamente identificados con material de abuso sexual infantil. Esta tecnología desarrollada y patentada por YouTube funciona de la siguiente manera: cuando un usuario sube un vídeo se crea con relación a este video un archivo de huella digital, un ID digital único o "hash" que, como ya se ha explicado anteriormente, representa el contenido del archivo de vídeo. Luego se envía dicho archivo mediante la API CSAI Match para compararlo con los demás archivos del repositorio de huellas digitales de

[83] Google (s.f.). *API Content Safety* Recuperado de https://protectingchildren.google/#tools-to-fight-csam
[84] Mathworks Inc. (s.f.). *Reconocimiento de imágenes con Machine Learning.* Recuperado de https://es.mathworks.com/discovery/image-recognition-matlab.html

YouTube. El repositorio contiene huellas digitales de contenido inadecuado previamente detectado por YouTube y Google. Si la coincidencia es positiva, se revisa manualmente el vídeo para verificar que contiene imágenes de abuso sexual infantil (Google, s.f.). [85]

La plataforma advierte en sus *Políticas de Privacidad*, que recopila el contenido que crea, carga o recibe, lo que incluye fotos y videos tal como lo especifica, de modo que cuando se utiliza el servicio se acepta dicha condición (YouTube, s.f.). [86]

¿Es posible pensar en un sistema de detección de CSAM desconocido que se realice de manera automática y sin supervisión humana?

La respuesta es sí. Las técnicas de Deep Learning pueden producir resultados más precisos que las técnicas de Machine Learning toda vez que el aprendizaje profundo utiliza modelos más complejos con parámetros que pueden "ajustarse" más estrechamente a los datos.

Tal como explica The MathWorks, Inc., Deep Learning puede aplicarse al reconocimiento de imágenes mediante el uso de una red neuronal convolucional para aprender automáticamente las características relevantes de las imágenes de entrenamiento e identificar automáticamente esas características en nuevas imágenes. Las redes neuronales convolucionales están diseñadas para extraer características de imágenes que frecuentemente dan como resultado precisiones de clasificación de última generación.[87]

El proceso de trabajo del Deep Learning para reconocimiento de imágenes implica:

1. Preparación de los datos de entrenamiento: se selecciona un un conjunto de imágenes y se las agrupa en las categorías correspondientes. Este paso también puede incluir tareas de preprocesamiento para mejorar la consistencia de las imágenes y lograr así un modelo más preciso.

[85] Google (s.f.). *kit de herramientas de seguridad infantil.* Recuperado de https://protectingchildren.google/intl/es-419/tools-for-partners/.
[86] YouTube (s.f.). *Proteger a los menores en riesgo.* Recuperado de https://www.youtube.com/howyoutubeworks/our-commitments/fostering-child-safety/#protecting-minors-at-risk
[87] Mathworks Inc. (s.f.). *Reconocimiento de imágenes con Deep Learning.* Recuperado de https://la.mathworks.com/campaigns/offers/next/machine-learning-vs-deep-learning.html

2. Creación de un modelo de Deep Learning: se puede desarrollar un modelo de Deep Learning desde cero, o se puede utilizar un modelo previamente entrenado como punto de partida.
3. Entrenamiento del modelo: implica presentar los datos de referencia al modelo. Luego, el modelo realiza varias iteraciones de los datos y aprende automáticamente las características más importantes de las imágenes provistas. A medida que se desarrolla el entrenamiento, el modelo aprende características más sofisticadas, hasta que logra distinguir con precisión las diferentes clases de imágenes.
4. Prueba: es necesario probar el modelo con datos nuevos que no se hayan analizado antes para ver cómo interpreta la imagen. Si los resultados no son los esperados, se debe seguir entrenando el modelo hasta lograr mayor precisión.

Para que un modelo produzca resultados más precisos, se debe utilizar los datos correctos. La selección de funciones permite garantizar que el modelo se centre en los datos con mayor poder predictivo y no se disperse con datos que no ayudarán a la toma de decisiones. La selección precisa de características dará como resultado un modelo más rápido y eficiente.[88]

La IA también permite la detección, prevención y mitigación del grooming on line. A continuación, se presentan algunos desarrollos:

Artemis de Microsoft

Esta tecnología patentada por Microsoft con el nombre clave “Project Artemis”, pero desarrollada en colaboración con The Meet Group, las plataformas de videojuegos en línea Roblox, Kik y Thorn ha logrado que los depredadores en línea que intenten atraer a los niños para propósitos sexuales puedan ser detectados, abordados y reportados.

Courtney Gregoire, Directora de Seguridad Digital de Microsoft, explica que, como empresa tecnológica, tienen la responsabilidad de crear software, dispositivos y

[88] Mathworks Inc. (s.f.). *Reconocimiento de imágenes con Deep Learning.* Recuperado de https://la.mathworks.com/campaigns/offers/next/machine-learning-vs-deep-learning.html

servicios que tengan funciones de seguridad integradas y aprovechar la tecnología al servicio para detectar, interrumpir y reportar contenido ilegal, incluida la explotación sexual infantil en línea (Courtney Gregoire, 2020).[89]

El proyecto comenzó en noviembre de 2018 y fue liderado por el doctor Hany Farid quien, en 2009, se asoció con Microsoft y el Colegio Dartmouth para el desarrollo de PhotoDNA. Con el propósito de ayudar a identificar instancias potenciales de grooming on line y poder dar una respuesta temprana efectiva, los equipos diseñaron esta técnica de machine learning aplicada a conversaciones de chat por texto que evalúa y califica las características de la conversación y asigna un valor de probabilidad, que luego, moderadores humanos deben corroborar para determinar si se trata o no de una inminente amenaza, en caso positivo reportar a las autoridades.

A partir del año 2020, el licenciamiento y la adopción de esta aplicación quedó a cargo de Thorn, sin embargo, se encuentra a disposición para que, otras compañías tecnológicas puedan involucrarse y realizar contribuciones y mejoras con el propósito de mejorarla y realizar ajustes que permita arrojar resultado con más autonomía y precisión.

Sweetie, la cazadora de pedófilos.

En 2014, el australiano Scott Robert Hansen se convirtió en el primer condenado gracias a "Sweetie", un proyecto sin precedentes creado por Terre des Hommes, una organización con sede en Holanda que lucha activamente contra la explotación infantil en el mundo. Sweetie es un avatar digital que fue diseñado para simular en apariencia y comportamiento a una niña filipina de 10 años, con el objetivo de captar y atrapar agresores sexuales de NNA en internet (Hans Guyt, 2014).[90]

Lo revolucionario de este prototipo radica en el uso de IA y otras tecnologías avanzadas, que permiten a Sweetie generar conversaciones, imágenes y videos como si

---

[89] Courtney Gregoire (2020). *Microsoft comparte nueva técnica para hacer frente al grooming infantil en línea para propósitos sexuales.* Recuperado de https://news.microsoft.com/es-xl/microsoft-comparte-nueva-tecnica-para-hacer-frente-al-grooming-infantil-en-linea-para-propositos-sexuales/

[90] Hans, Guyt (22/10/2014). *Sweetie pone a pedosexual tras las rejas.* Terre des Hommes. Recuperado de https://www.tdh.de/was-wir-tun/arbeitsfelder/sexuelle-gewalt/meldungen/sweetie-verurteilung-paedosexueller/

se estuviera interactuando con una niña real. Al principio, las conversaciones por chat eran realizadas por operadores. Luego, se logró automatizar con la utilización de bots y más tarde, las respuestas de Sweetie fueron entrenadas mediante aprendizaje automático. Pera la reproducción de videos se utilizó *motion capture*, una tecnología capaz de captar los movimientos y la voz de una persona y replicarla en un entorno virtual, la misma que se utilizó para hacer Gollum en la película El Señor de los Anillos.

Tras su creación, "Sweetie" fue introducida en sitios de la deep web dedicados a promover el abuso sexual de menores. Patricia Peiró, en una nota publicada en el periódico on line "El País" explica que, cuando pusieron en funcionamiento a "Sweetie", en tan solo diez semanas se contactaron más de 20.000 hombres procedentes de 71 países lo que demostró que se trataba de un problema global. Peiró refiere también que, el hecho de que esta iniciativa naciera en Holanda no es casual ya que, según un informe anual de Unicef publicado en entonces, Holanda es número uno de los cinco países que acumulan el 92% de las webs pedófilas en el mundo (Peiró, 2018).[91]

¿Por qué se pensó en una niña filipina? La organización Terre des Hommes explica que, a cambio de sexo virtual, hombres ricos pagan a niños de países pobres generalmente del Sudeste asiático y África. El turismo sexual infantil on line es un fenómeno que crece cada vez más, agrega (Terre des Hommes, 2014, 1m27s).[92]

Al interactuar en línea a través de chats y otras plataformas digitales, Sweetie recolecta información de los agresores como el nombre de usuario, ubicaciones geográficas y direcciones IP. En el caso de Hansen, la información obtenida fue clave para lograr su condena, marcando un precedente ya que fue la primera vez que un tribunal condenó a un pedófilo con pruebas obtenidas de esta manera. Desde su creación, más de mil depredadores fueron identificados en muy poco tiempo.

El caso de Sweetie es un ejemplo claro de cómo la IA y la tecnología pueden ser empleadas de manera efectiva para combatir los delitos contra la integridad sexual de

---

[91] Peiró, Patricia (27/02/2018). *Sweetie, la cazadora de pedófilos que quiere colaborar con la policía.* EL PAIS. Recuperado de https://elpais.com/elpais/2018/02/15/planeta_futuro/1518696623_728007.html

[92] Terre des Hommes (2014). SWEETIE - *Terre des hommes gegen Kinderprostitution.* Recuperado de https://www.youtube.com/watch?v=wObUgUlI4YU&list=PLx8n7ozHKB2yTgvXSnaX89JKUn9ks3mWg

NNA en internet. Esta herramienta ha abierto nuevas posibilidades demostrando que la tecnología puede desempeñar un papel crucial en la investigación de estos crímenes y la identificación de sus autores.

Sin embargo, el uso de avatares digitales como Sweetie ha planteado debates éticos en torno a la privacidad, la intimidad y la protección de datos personales al recopilar información sensible sin el consentimiento explícito de los involucrados.

Este tipo de prácticas plantea interrogantes sobre los límites legales y morales de la vigilancia digital. Si hacemos una analogía con nuestra normativa procesal, para ingresar en un domicilio o intervenir una comunicación telefónica, se requiere una orden judicial debidamente fundada, respaldada por una justificación clara, basada en indicios suficientes de que en ese lugar o en dicha comunicación se podrían encontrar pruebas vinculadas a un hecho delictivo.

De manera similar, el uso de tecnologías como Sweetie debería estar sometido a un marco normativo que garantice el equilibrio entre la protección de derechos individuales y la eficacia en la prevención del crimen, respetando los principios del debido proceso y el control judicial en la obtención de pruebas.

Clearview AI

Clearview AI es una compañía tecnológica fundada en 2017 por Hoan Ton-That, un empresario australiano-estadounidense que desarrolló una herramienta de reconocimiento facial que permite, a través de redes neuronales, identificar a personas a partir de fotos o imágenes públicas, extraídas de diversas fuentes de Internet, como redes sociales o sitios web.

Clearview AI utiliza algoritmos de reconocimiento facial para analizar características únicas de los rostros, como la distancia entre los ojos, la forma de la nariz o la estructura facial, y luego busca coincidencias en su base de datos. Esta base de datos se ha formado recolectando imágenes de millones de sitios web de manera automatizada, y el software puede comparar una imagen dada con millones de otras

en cuestión de segundos. Si encuentra una coincidencia, proporciona información sobre la fuente de la imagen, lo que permite identificar a la persona en cuestión.

En mayo de año 2019, National Center for Missing and Exploited Children (NCMEC) recibió un informe de Yahoo, Inc. indicando que un usuario recibió imágenes que mostraban abusos sexuales a una niña. En una de las imágenes podía visualizarse la cara de un adulto. La agencia federal Homeland Security Investigations (HSI) del Departamento de Seguridad Nacional de los EEUU solicitó ayuda a Clearview AI para investigar el hecho. Clearview AI, utilizando el reconocimiento facial encontró que el mismo rostro aparecía en el fondo de una imagen que alguien había subido a Internet, foto tomada en una feria comercial. Esto permitió a los detectives extraer dos pistas importantes: la ubicación de la feria y el nombre de la marca que representaba. Con esta información, los investigadores se constituyeron en el lugar, entrevistaron al empleador y obtuvieron el nombre del sospechoso, que junto a otras pruebas confirmatorias ayudaron a dar con el sujeto y proceder a su detención. El 7 de junio de 2019, las fuerzas del orden federales arrestaron al agresor. Se trataba de Andrés Rafael Viola, de 36 años en aquel entonces, un ciudadano argentino que residía en Las Vegas, Nevada mientras que la víctima era una niña de 7 años que estaba bajo su cuidado la que fue rescatada. Un examen forense de los dispositivos electrónicos que fueron secuestrados en la casa de Viola reveló casi 350 imágenes y videos con material de abuso sexual de NNA, incluida la explotación sexual de la víctima que fue rescatada. El agresor había utilizado la red oscura para distribuir, intercambiar y compartir el material de abuso sexual producido con la menor que tenía a cargo. Viola fue condenado a 35 años de prisión por abuso sexualmente en reiteradas ocasiones, producción, tenencia y distribución de imágenes y videos de abuso sexual infantil (U.S. Attorney's Office, District of Nevada, 2020).[93]

Clearview AI no sólo ha ayudado a identificar agresores sino también a muchas víctimas, dado que el escenario de estos delitos contra la integridad sexual de NNA es Internet. La tarea de identificación de las víctimas sin esta tecnología podría llevar días

[93] U.S. Attorney's Office, District of Nevada (16 de septiembre de 2020). *Argentine Citizen Sentenced To 35 Years In Prison For Child Sexual Exploitation And Distribution Of Child Pornography Over The Dark Web.* U.S. Department of Justice. Recuperado de https://www.justice.gov/usao-nv/pr/argentine-citizen-sentenced-35-years-prison-child-sexual-exploitation-and-distribution

o incluso más tiempo y ser demasiado tarde para encontrarlas y rescatarlas, explica Metcalf Kevin, Presidente y fundador de National Child Protection Task Force (Clearview AI, 2022, 05m10s).[94]

A pesar de que Clearview AI asegura que solo ofrece sus servicios a agencias gubernamentales, fuerzas de seguridad y organismos de investigación, su uso ha generado preocupación en cuanto a la privacidad y la protección de datos personales enfrentado críticas importantes por parte de defensores de la privacidad, organizaciones de derechos humanos y gobiernos. El principal motivo de preocupación es que la recolección masiva de imágenes faciales sin el consentimiento de los individuos podría violar leyes de privacidad en varios países. Varias demandas y acciones legales se han presentado contra la empresa, cuestionando la legalidad de su método de obtención de datos y el posible mal uso de la tecnología.

Además, algunos críticos argumentan que el software podría ser susceptible de errores, lo que podría llevar a identificar falsamente a personas inocentes. Esto ha encendido debates sobre el equilibrio entre el uso de tecnología avanzada para la seguridad pública y la protección de los derechos individuales. En conclusión, el uso de esta tecnología de (IA) también requiere regulación.

AI Act

El Reglamento de Inteligencia Artificial de la Unión Europea (conocido como AI Act) es una propuesta normativa presentada por la Comisión Europea en abril de 2021, que busca establecer un marco regulador para los países miembros de la Unión Europea (en adelante UE) con el propósito de garantizar que la IA se desarrolle y utilice de manera ética, segura y respetuosa con los derechos fundamentales. En sintonía, la Comisión propone los siguientes objetivos específicos:

- Garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;

[94] Clearview AI (2022). *How Facial Recognition is Identifying Human Trafficking Victims.* Recuperado de https://www.youtube.com/watch?v=1G5hW1ZIHCg

- Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;
- Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;
- Facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado. (AI Act, 2021).[95]

La AI Act plantea un marco regulatorio según el riesgo que presentan los sistemas de IA, y lo clasifica en:

1.Riesgo inaceptable: refiere a los usos de la IA que se consideran una amenaza para la seguridad y los derechos fundamentales estableciendo que, estarán prohibidas las prácticas de inteligencia artificial que se sirvan de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra; que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental o que sean utilizados por las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas como el sistema de "puntuación social" aplicado por el gobierno en China, donde los comportamientos de los ciudadanos son evaluados y calificados con posibles consecuencias negativas.

También prohíbe el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público salvo y en la medida en que dicho uso sea estrictamente necesario para la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; la prevención de una amenaza específica,

[95] Comisión Europea (21/04/2021). *Ley de Inteligencia Artificial de la UE.* Recuperado de https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista y excepcionalmente para la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido un delito teniendo en cuenta las condiciones impuestas en el inc. 2. (AI Act, 2021, art.5 inc.1).[96]

2.Riesgo alto: refiere a las tecnologías de IA que podrían afectar derechos fundamentales, los sistemas que influyen en la toma de decisiones judiciales, la IA utilizada en selección de personal, educación, o servicios financieros.

Las empresas que desarrollen o utilicen IA de "alto riesgo" estarán sujetas a auditorías y deberán cumplir con una serie de obligaciones legales, como garantizar la transparencia de los algoritmos y llevar un registro de las decisiones que toma la IA. Se establecerán mecanismos de control y sanciones significativas para quienes incumplan las regulaciones.

3.Riesgo limitado: incluye sistemas de IA que requieren cierto nivel de transparencia, como los chatbots o los asistentes virtuales. En estos casos, los usuarios deben ser informados cuando están interactuando con una IA.

4.Riesgo mínimo o nulo: esta categoría abarca la mayoría de los sistemas de IA, como los videojuegos y aplicaciones básicas, que tienen pocas restricciones.

Como se mencionó, uno de los objetivos principales es el respeto por los derechos fundamentales y en este sentido incluye la no discriminación, por ello, la regulación incluye disposiciones para evitar la creación de algoritmos sesgados y garantizar la equidad en el uso de sistemas de IA.

El art. 13 refiere al deber de transparencia y comunicación de información a los usuarios y el art. 16 y ss del capítulo 3 establece las obligaciones de los proveedores, representantes, importadores, distribuidores y usuarios de sistemas de IA.

Pero no todo es restricción. La propuesta normativa apoya la innovación y promueve la creación de "espacios de prueba" (regulatory sandboxes) para que las empresas puedan desarrollar sistemas de IA en un entorno controlado e incentiva el

[96] Comisión Europea (21/04/2021). *Ley de Inteligencia Artificial de la UE.* Recuperado de https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

desarrollo de IA confiable, especialmente en sectores como la salud, la energía o el transporte (AI Act, 2021, art. 53).[97]

En conclusión, la AI Act posiciona a Europa como líder mundial en la regulación ética y segura de la IA, con miras a crear un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales, promoviendo un desarrollo responsable de la IA.

La AI Act complementa otras normativas europeas, como el Reglamento General de Protección de Datos (GDPR), que regula el uso y tratamiento de datos personales, y la Ley de Servicios Digitales (Digital Services Act - DSA), que busca garantizar un entorno digital más seguro y responsable. Juntas, estas leyes proporcionan un marco regulatorio integral que cubre tanto los aspectos tecnológicos como los derechos y libertades de los ciudadanos europeos.

En Argentina

Si bien nuestro país no cuenta aún con una ley que regule la IA, se han dado algunos avances y propuestas legislativas en los últimos años. Estos intentos buscan establecer un marco normativo para regular el uso la de IA con miras a proteger los datos personales, la transparencia algorítmica y los derechos fundamentales.

Como normativas que le preceden, contamos con la Ley 25.326 de Protección de Datos Personales que, si bien no regula con relación a la IA, es relevante para su uso ya que la mayoría estos sistemas utilizan el procesamiento masivo de datos, entre ellos datos personales. La Ley 25.326, sancionada en el año 2000, establece las condiciones para la recopilación, almacenamiento y uso de datos personales, así como los derechos de los titulares de dichos datos. Sin embargo, debido a que la ley fue promulgada antes del surgimiento de la IA se ha indicado la necesidad de actualizarla (Ley N.º 25.326, 2000).[98]

---

[97] Comisión Europea (21/04/2021). *Ley de Inteligencia Artificial de la UE.* Recuperado de https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[98] Ministerio de Justicia y Derechos Humanos de la Nación. (2000). *Ley N.º 25.326; Ley de Protección de los Datos Personales.* Boletín Oficial de la República Argentina.

En consecuencia, en el año 2022, la Agencia de Acceso a la Información Pública de Argentina lanzó un proceso de consulta pública para adaptarla a los nuevos desafíos tecnológicos, incluyendo la inteligencia artificial. Este proyecto de reforma también busca armonizar la legislación nacional con normativas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, e incluir temas como el consentimiento, los derechos sobre los datos y el uso de datos personales por parte de sistemas automatizados, sin embargo, a la fecha no se ha sancionado una nueva ley.

Se espera que, en los próximos años, Argentina avance hacia la creación de un marco regulatorio más específico para la IA. Esto incluiría no solo la protección de datos personales, sino también la regulación de los derechos de los usuarios frente a las decisiones automatizadas, la transparencia de los sistemas y las responsabilidades de las empresas que desarrollan IA.

En junio de 2023, la Subsecretaría de Tecnologías de la Información de la Jefatura de Gabinete de Ministros, dispuso las *Recomendaciones para una Inteligencia Artificial Fiable*. Se trata de "herramientas para proteger los derechos fundamentales, prevenir o disminuir los riesgos, promover la innovación y el diseño centrado en las personas" (Subsecretaria de Tecnologías de la Información, 2003).[99]

Tal como lo establece, estas herramientas están dirigidas a quienes llevan adelante proyectos de innovación pública que importen el uso de inteligencia artificial.

En dicho instrumento se transcribe los principios que la Organización de Naciones Unidas (ONU) a través de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) incluyó en la *Recomendación sobre la Ética de la Inteligencia Artificial*, a la que adhirieron todos los países miembros en la Asamblea General de noviembre de 2021, entre los cuales se encuentra Argentina. En resumen, estos principios son:

- **Proporcionalidad e inocuidad:** implica que, si potencialmente pudiera producirse un daño para los seres humanos, el medio ambiente o los

[99] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

ecosistemas, se debe garantizar la aplicación de procedimientos de evaluación de riesgos y la adopción de medidas para impedir que dicho daño se produzca.

- **Seguridad y protección:** establece que los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deberían ser evitados y deberían tenerse en cuenta, prevenirse y eliminarse a lo largo del ciclo de vida de los sistemas de IA para garantizar la seguridad y la protección de los seres humanos, del medio ambiente y de los ecosistemas.
- **Equidad y no discriminación:** Los actores de la IA deberían hacer todo lo razonablemente posible por reducir y evitar resultados discriminatorios o sesgados, promoviendo la diversidad y la inclusión, garantizando la justicia social y la equidad, de conformidad con el derecho internacional.
- **Sostenibilidad.** Implica que debería llevarse a cabo con pleno conocimiento de las repercusiones de dichas tecnologías en la sostenibilidad la evaluación continua de los efectos humanos, sociales, culturales, económicos y ambientales de las tecnologías de la IA.
- **Derecho a la intimidad y protección de datos:** para que se recopilen, utilicen, compartan, archiven y supriman de forma consistente con el derecho internacional y respetando al mismo tiempo los marcos jurídicos nacionales, regionales e internacionales pertinentes.
- **Supervisión y decisión humanas.** Puede ocurrir que, en algunas ocasiones, los seres humanos decidan depender de los sistemas de IA por razones de eficacia, pero la decisión de ceder el control en contextos limitados seguirá recayendo en los seres humanos, ya que estos pueden recurrir a los sistemas de IA en la adopción de decisiones y en la ejecución de tareas, pero un sistema de IA nunca podrá reemplazar la responsabilidad final de los seres humanos y su obligación de rendir cuentas.
- **Transparencia y explicabilidad:** las personas deberían tener la oportunidad de solicitar explicaciones e información al responsable de la IA o a las instituciones del sector público correspondientes. Estos informar y rendir cuentas, además de elaborarse mecanismos adecuados de supervisión, evaluación del impacto, auditoría y diligencia debida.

- **Sensibilización y educación:** mediante una educación abierta y accesible, la participación cívica, las competencias digitales y la capacitación en materia de IA, teniendo en cuenta la diversidad lingüística, social y cultural existente, a fin de garantizar una participación pública efectiva.
- **Gobernanza y colaboración adaptativas de múltiples partes interesadas:** implica la participación de los diferentes sectores para garantizar enfoques inclusivos en la gobernanza de la IA, entre estos los gobiernos, la comunidad técnica, la sociedad, los investigadores, los medios de comunicación, los educadores, las empresas del sector privado, las instituciones de derechos humanos, entre otros.[100]

Para diseñar un proyecto de innovación basado en el uso de la IA para la detección, prevención y mitigación de delitos contra la integridad sexual de NNA en internet, se debería tener en cuenta las recomendaciones sugeridas en este documento, no sólo con respecto a los principios a observar, sino también con relación a los aspectos éticos a considerar en cada una de las etapas del diseño.

Seguidamente, se detallan las etapas del diseño y los aspectos a tener en cuenta que sugiere las *Recomendaciones para una Inteligencia Artificial Fiable.*

Etapa N°1: Diseño y modelado de datos: es fundamental en esta primera etapa acordar de manera clara el propósito del proyecto, según refiere. En las recomendaciones se remarca también la importancia de que se incluyan como criterios de diseño aspectos éticos ya que facilitarán el cumplimiento de los principios definidos y aumentarán en consecuencia las probabilidades de éxito del proyecto. Cabe recordar que los principios definidos por la UNESCO deben ser aplicados en la etapa de diseño como así también en la de desarrollo, implementación y uso ético de la IA (Subsecretaria de Tecnologías de la Información, 2003).[101]

También dispone que debe tenerse en cuenta en esta primera fase de diseño, los perfiles de personas destinatarias y las necesidades a cubrir. Además, debe analizarse

[100] UNESCO (2001). *Recomendación sobre la Ética de la Inteligencia Artificial*.
[101] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

las implicancias y el impacto en la sociedad en general, como así también los potenciales riesgos evaluados por nivel de impacto y probabilidad de ocurrencia y los tratamientos definidos para cada uno de ellos (Subsecretaria de Tecnologías de la Información, 2003).[102]

La clasificación de los datos y las fuentes es otro aspecto a tener en cuenta, según se establece en las recomendaciones y explica que los datos son la materia prima para construir el modelo entrenado de inteligencia artificial que se utilizará para que, al ingresar diferentes entradas, se obtenga una respuesta correcta. En consecuencia, la calidad de los datos que se utilicen determinará no solamente la calidad del modelo entrenado, sino que también contribuirá con el éxito del proyecto (Subsecretaria de Tecnologías de la Información, 2003).[103]

Etapa N°2: Verificación/Validación: en esta fase se cotejan de los diseños realizados en la primera etapa, teniendo en cuenta tanto los principios definidos por la UNESCO, como la interacción de las personas destinatarias con los prototipos diseñados, en condiciones similares a las que tendrá su implementación definitiva. En esta prueba con prototipos, se validarán diversos aspectos éticos, tales como la congruencia entre los resultados y las expectativas del diseño, la ausencia de sesgos, la explicabilidad del modelo, y otros elementos éticos del diseño que puedan ser susceptibles de mejora (Subsecretaria de Tecnologías de la Información, 2003).[104]

El documento establece que los conjuntos de datos creados específicamente para entrenar modelos de inteligencia artificial también deben ser validados antes de su implementación en el campo. En este sentido, los profesionales del equipo especializados en ciencias de datos serán los responsables de evaluar la calidad de los datos que se utilizarán para entrenar los modelos de IA (Subsecretaria de Tecnologías de la Información, 2003).[105]

---

[102] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.
[103] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.
[104] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.
[105] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

En relación con los principios de la UNESCO mencionados anteriormente, se sugiere establecer una clasificación de riesgo (como un sistema de tres niveles tipo semáforo, o con una escala del uno al cinco) para evaluar en qué medida se ajustan o se ven comprometidos Finalmente agrega que se deberá utilizar un medio de registro formal que permita realizar la trazabilidad y auditorías de todas y cada una de las acciones de verificación y validación (Subsecretaria de Tecnologías de la Información, 2003).[106]

Etapa N°3: Implementación: dispone que, se deberá garantizar que la implementación sea en un marco adecuado de seguridad de la información teniendo en cuenta los estándares y normativas internacionales, así como con las regulaciones locales. A tal efecto, se deben realizar pruebas periódicas para detectar posibles vulnerabilidades de seguridad. En esta fase, además propone realizar trazabilidad sobre las acciones y decisiones ocurridas en el proyecto, realizar auditorías y ofrecer al usuario facilidades de accesibilidad a las tecnologías de información y comunicaciones (TIC). (Subsecretaria de Tecnologías de la Información, 2003).[107]

Etapa N°4: Operación y mantenimiento: establece que los proyectos de innovación tecnológica no terminan con la implementación, sino que la operación y mantenimiento constituyen la etapa final del ciclo de vida de la IA. En este sentido, el monitoreo es una acción que se realiza en esta etapa para asegurarse de que todo funcione conforme lo esperado, detectar otro tipo de resultados indeseables que, de no ser monitoreados, podrían tener distintos grados de impacto negativo o perjudicial en las personas. En esta fase también permite corroborar si se receptaron los principios y recomendaciones incluidas en el documento y si se poseen las bases mínimas para poder brindar un correcto tratamiento ante un eventual incidente ético (Subsecretaria de Tecnologías de la Información, 2003).[108]

---

[106] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.
[107] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.
[108] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

Con respecto al mantenimiento, las recomendaciones hacen referencia tanto de la infraestructura donde se despliega la solución tecnológica basada en IA, así como también del propio modelo explicando que muchas veces estos se degradan y dejan de responder de manera correcta, agregando que dichas acciones permiten que exista disponibilidad, continuidad, y sostenibilidad del servicio prestado a través de la solución de IA (Subsecretaria de Tecnologías de la Información, 2003).[109]

Las *Recomendaciones para una Inteligencia Artificial Fiable* son un marco que guía el desarrollo de proyectos de innovación pública que implique el uso de inteligencia artificial. Sin embargo, debería precederle una normativa general que regule el uso y desarrollo de la IA en nuestro país.

Conclusión y postura de la autora

Vivimos un momento sin precedentes en la historia de la humanidad: internet es parte de nuestras vidas y la IA llegó para quedarse, a la vez que su desarrollo y aplicaciones parecen no tener fronteras.

Sin duda, la IA tiene el potencial de contribuir a la detección, prevención y mitigación de delitos contra la integridad sexual de NNA en internet. Su aplicación en los precedentes mencionados ha demostrado ser de gran ayuda para identificar CSAM mediante algoritmos de reconocimiento de imágenes y al monitorear las redes sociales, aplicaciones y plataformas digitales, la IA puede advertir también patrones de comportamiento asociados con el ciberacoso mediante algoritmos de procesamiento de lenguaje natural (PNL).

La calidad de los datos y el entrenamiento adecuado de los modelos de aprendizaje automático son claves para que la IA logre los resultados esperados, de lo contrario, los errores derivados de datos incorrectos o sesgados pueden generar resultados inexactos y hasta discriminatorios. En otras palabras, el éxito de los resultados dependerá de cuán entrenado esté el modelo y su entrenamiento dependerá de los datos introducidos. El avance de la ciencia y de la tecnología puede

[109] Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

ofrecer modelos más autónomos y precisos, como aquellos basados en redes neuronales artificiales.

Sin embargo, el uso de la IA también plantea desafíos importantes en términos de afectación de derechos fundamentales, como el derecho a la privacidad, la protección de datos personales y la no discriminación.

La recopilación, almacenamiento y procesamiento de datos personales genera serias preocupaciones en torno a la privacidad y la seguridad de los usuarios mientras que la vigilancia masiva, el monitoreo y el análisis automático de contenido y de las conversaciones privadas puede ser intrusivo y vulnerar la privacidad y la intimidad de las personas. En este sentido es fundamental que los usuarios sean informados y brinden su consentimiento, pero además es necesario que se garantice procesos adecuados para la protección de datos y la seguridad de la información.

Por otra parte, la utilización de CSAM (*child sexual abuse material*) identificado para el entrenamiento de los modelos de IA implica un delicado balance ético entre la utilidad de esta información y el respeto por las víctimas.

Nuestro país carece todavía de una regulación específica que establezca un marco jurídico claro para el desarrollo y la aplicación de la IA. La falta de legislación que norme el uso ético y seguro deja un vacío legal que puede derivar en la utilización indiscriminada de estas tecnologías y la afectación de derechos fundamentales.

Es urgente que Argentina avance en la elaboración de normativas adecuadas, alineadas con estándares internacionales, para garantizar que el desarrollo de la IA respete los derechos fundamentales de los individuos y promueva un uso responsable y ético de estas herramientas. La Ley de Inteligencia Artificial propuesta por la Comisión Europea es un precedente que puede tomar como modelo y al mismo tiempo armonizar las regulaciones lo que facilitaría la cooperación internacional.

Ante situaciones de conflicto entre derechos fundamentales se deberá aplicar el principio de ponderación, evaluando qué derechos deben prevalecer en cada caso particular. Personalmente considero que la protección de los NNA debe ser prioritaria, atento a su condición de mayor vulnerabilidad es que requiere especial protección.

Así, la Convención sobre los Derechos del Niño y diversas normativas nacionales e internacionales establecen que el interés superior del niño debe guiar todas las decisiones que les afecten.

No obstante, la herramienta más poderosa para combatir los delitos contra la integridad sexual de NNA en internet sigue siendo la educación. Capacitar a los NNA, padres, tutores y educadores para una navegación segura es clave, promover la concientización sobre los peligros en línea y fortalecer las capacidades para responder ante posibles escenarios de riesgo resulta fundamental.

La IA puede ser una aliada poderosa, pero sin una acción conjunta y coordinada, sus beneficios quedarían limitados. En este sentido, el compromiso de todos (familias, instituciones educativas, empresas y autoridades) es esencial para construir un futuro digital seguro para los NNA.

Es real, la tecnología avanza a pasos agigantados, pero no debemos olvidar el respeto por los derechos fundamentales. La educación, la colaboración y la regulación adecuada son las claves para lograr este equilibrio.

El futuro de la tecnología y el bienestar de los NNA dependen de cómo elegimos usar y regular las herramientas hoy.

Referencias

Legislación

Ley N° 23849 (1990). *Convención sobre los Derechos del Niño*. Boletín Oficial de la República Argentina.

Ley N° 23849 (1990). *Convención sobre los Derechos del Niño*. Boletín Oficial de la República Argentina.

Ley N° 24430 (1994). *Constitución Nacional.* Boletín Oficial de la República Argentina.

Ley N° 26.904. (2013). *Modificación del Código Penal e incorporación del artículo 131 sobre ciberacoso o grooming.* Boletín Oficial de la República Argentina.

Ley N° 27.436 (2018). *Modificación del art. 128 del Código Penal.* Boletín Oficial de la República Argentina.

Naciones Unidas (2000). *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.*

Naciones Unidas (2000). *Convención contra la Delincuencia Organizada Transnacional*.

Convenio de Budapest. (2001). *Convenio sobre la ciberdelincuencia*. Preámbulo.

Ley N° 25.632 (2002). *Convención Internacional contra la Delincuencia Organizada Transnacional.* Boletín Oficial de la República Argentina.

Ley N° 26.061 (2005). *Protección Integral de los Derechos de la Niñas, Niños y Adolescentes*. Boletín Oficial de la República Argentina.

Ley N° 26.388 (2008). Delitos Informáticos y Ciberseguridad. Boletín Oficial de la República Argentina.

Ley N° 27.590. (2020). *Ley Mica Ortega sobre la prevención y concientización del ciberacoso o grooming.* Boletín Oficial de la República Argentina.

Convenio de Budapest (2021). *Convenio sobre Ciberdelito*. Ley 27411/2017. Boletín Oficial de la República Argentina.

Comisión Europea (2021). *Ley de Inteligencia Artificial de la UE*. *Reglamento del Parlamento Europeo y del Consejo.*

Subsecretaria de Tecnologías de la Información (2003). *Disposición 2/2023. Recomendaciones para una Inteligencia Artificial Fiable.* Boletín Oficial de la República Argentina.

Libros

Aboso, G. E. (2020). *DERECHO PENAL CIBERNÉTICO.* Editorial B de F.

Cabrera, L. (2020). *Protección infantil en entornos digitales: Prevención y educación frente a riesgos en internet.* Buenos Aires: Editorial Kapelusz.

Chamorro Concha, Gabriela (2021). CIBERCRIMEN II, Derecho procesal Penal. *Material de explotación sexual infantil y la importancia de las investigaciones en redes.* BdeF Editorial

Corvalán J. G. y Ciraudo D. (2021). *CIBERCRIMEN II, Capítulo IV: Inteligencia Artificial aplicada al Derecho penal y procesal penal.* Editorial B de F.

Mauri, Miriam C. (2019). *CIBERDELITOS*, Capítulos VI. Editorial Hammurabi.

Riquet, Fabián Luis (2019). *CIBERDELITOS*, Capítulos VII. Editorial Hammurabi.

Publicaciones/Informes/Reportes

Alan Turing (1950) Computing Machinery and Intelligence. Oxford Academic. Recuperado de https://academic.oup.com/mind/article/LIX/236/433/986238

Carnaghi Cintia et al. (2022). *Ciberdelitos durante la pandemia del covid-19 en Argentina.* Ministerio de Justicia y DD. HH de la Nación.

ECPAT International (2016) *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.* Recuperado de https://ecpat.org/luxembourg-guidelines/

GEGENHEIMER Scott et al (2019). *Seguridad de los niños en línea: minimizando el riesgo de la violencia, el abuso y la explotación en línea.* UNESCO. Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000374580

Giulia Testa, Alejandro Villena, Gemma Mestre y Carlos Chiclana. (2023). *Guía para familias adolescentes y uso de pornografía.* UNIR. Recuperado de

https://www.unir.net/wp-content/uploads/2023/12/Guia-para-Familias_Adolescentes-y-Uso-de-Pornografia.pdf

John McCarthy. (2007). *WHAT IS ARTIFICIAL INTELLIGENCE?* Computer Science Department, Stanford University. Recuperado de https://www-formal.stanford.edu/jmc/whatisai.pdf

Paolini, P., & Ravalli, M. J. (2016). Investigación sobre percepciones y hábitos de niños, niñas y adolescentes en internet y redes sociales. UNICEF. Recuperado de https://www.unicef.org/argentina/media/1636/file/Kids-online.pdf

Statista Research Department. (2024). *Argentina: porcentaje de población con acceso a internet, por edad 2023.* Recuperado de *https://es.statista.com/estadisticas/1220202/porcentaje-poblacion-acceso-internet-edades-argentina/*

Susan Jasper (2022). *Cómo detectamos, eliminamos y denunciamos el material de abuso sexual infantil.* Recuperado de https://blog.google/intl/es-es/productos/informacion/2022_10_como-detectamos-eliminamos-y/

Unicef (2015). *Directrices de Protección de la Infancia en Línea para la Industria.* Recuperado de https://www.unicef.org/dominicanrepublic/media/916/file/Publicaci%C3%B3n%20%7C%20Directrices%20de%20proteccion%20de%20la%20infancia%20en%20linea%20para%20la%20industria.pdf

Unicef (2020). *Google y UNICEF revelan cuáles son las preocupaciones de adolescentes, familias y docentes sobre el uso de la tecnología.* Recuperado de https://www.unicef.org/argentina/comunicados-prensa/google-y-unicef-revelan

-datos-internet-segura#:~:text=El%20tema%20que%20m%C3%A1s%20les,ciber
n%C3%A9tico%20est%C3%A1%20en%20segundo%20puesto.

Noticias/Artículos periodísticos

BBC Mundo (5 de agosto de 2014) *Por qué Google está revisando los correos de Gmail.* Recuperado de https://www.bbc.com/mundo/noticias/2014/08/140805_google_pornografia_gmail_am

CNN (21 de abril de 2014). *¿Cómo funciona el reconocimiento facial de Facebook?* Recuperado de https://cnnespanol.cnn.com/2014/04/21/como-funciona-el-reconocimiento-facial-de-facebook

Banafa Ahmed (14 de octubre 2022). *Intellectual Abilities of Artificial Intelligence.* Spark BBVA. Recuperado de https://www.bbvaspark.com/contenido/en/news/intellectual-abilities-of-artificial-intelligence/

Infobae (2024). *El crimen de Micaela Ortega, la nena de 12 años cuyo caso impulsó la ley de grooming.* Recuperado de https://www.infobae.com/sociedad/2021/08/04/el-crimen-de-micaela-ortega-la-nena-de-12-anos-cuyo-caso-impulso-la-ley-de-grooming/

Boscovich R. (7 sept 2016) PhotoDNA: *Así es la herramienta que atrapa a los pederastas en Internet.* Recuperado de

https://www.elmundo.es/economia/2016/09/07/57cd61f946163f30748b45d7.html

Interpol (8 de noviembre de 2019). *La base de datos de INTERPOL permite identificar a menores víctimas de delitos sexuales.* Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2019/La-base-de-datos-de-INTERPOL-permite-identificar-a-menores-victimas-de-delitos-sexuales

Lewis Glyn. (14 de abril de 2015) *La tecnología de Microsoft impulsa la labor mundial de identificación -a través de INTERPOL- de niños víctimas de abusos.* INTERPOL. Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2015/La-tecnologia-de-Microsoft-impulsa-la-labor-mundial-de-identificacion-a-traves-de-INTERPOL-de-ninos-victimas-de-abusos

Moran Mick (14 de abril de 2015) *La tecnología de Microsoft impulsa la labor mundial de identificación -a través de INTERPOL- de niños víctimas de abusos.* Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2015/La-tecnologia-de-Microsoft-impulsa-la-labor-mundial-de-identificacion-a-traves-de-INTERPOL-de-ninos-victimas-de-abusos

Peiró, Patricia (27/02/2018). *Sweetie, la cazadora de pedófilos que quiere colaborar con la policía.* EL PAIS. Recuperado de https://elpais.com/elpais/2018/02/15/planeta_futuro/1518696623_728007.html

U.S. Attorney's Office, District of Nevada (16 de septiembre de 2020). Argentine Citizen Sentenced To 35 Years In Prison For Child Sexual Exploitation And Distribution Of Child Pornography Over The Dark Web. U.S. Department of Justice. Recuperado de https://www.justice.gov/usao-nv/pr/argentine-citizen-sentenced-35-years-prison-child-sexual-exploitation-and-distribution

Sitios Web

Arend Hintze. (s.f.). *Tipos de inteligencia artificial.* Tableau. Recuperado de https://www.tableau.com/es-mx/data-insights/ai/tipos-de-inteligencia-artificial

Centro de Información Jurídica. (2016). *Operación Ángel Guardián.* Ministerio Público Provincia de Buenos Aires. Recuperado de https://www.mpba.gov.ar/novedad/515

Child Rights International Network (2023). *Explicando la tecnología para detectar abuso sexual infantil online.* Recuperado de https://home.crin.org/readlistenwatch/stories/explainer-detection-technologies-child-sexual-abuse-online

Courtney Gregoire (2020). *Microsoft comparte nueva técnica para hacer frente al grooming infantil en línea para propósitos sexuales.* Recuperado de https://news.microsoft.com/es-xl/microsoft-comparte-nueva-tecnica-para-hacer-frente-al-grooming-infantil-en-linea-para-propositos-sexuales/

Google (s.f.). *Voice Match.* Recuperado de https://support.google.com/chromecast/answer/9071681?hl=es&co=GENIE.Platform%3DAndroid

Google (s.f.). *Política sobre seguridad infantil.* Recuperado de https://support.google.com/youtube/answer/2801999?hl=es

Google (s.f.). *API Content Safety* Recuperado de https://protectingchildren.google/#tools-to-fight-csam

Google (s.f.). *kit de herramientas de seguridad infantil.* Recuperado de https://protectingchildren.google/intl/es-419/tools-for-partners/.

Hans Guyt (22/10/2014). *Sweetie pone a pedosexual tras las rejas.* Terre des Hommes. Recuperado de https://www.tdh.de/was-wir-tun/arbeitsfelder/sexuelle-gewalt/meldungen/sweetie-verurteilung-paedosexueller/

IBM. (s.f.). *What is artificial intelligence (IA)?* Recuperado de https://www.ibm.com/es-es/topics/artificial-intelligence?mhsrc=ibmsearch_a&mhq=inteligencia%20artificial

IBM. (s.f.). *What is machine learning?* Recuperado de https://www.ibm.com/topics/machine-learning#:~:text=Machine%20learning%20(ML)%20is%20a,learn%2C%20gradually%20improving%20its%20accuracy.

IBM. (s.f.). *What is deep learning?* Recuperado de https://www.ibm.com/es-es/topics/deep-learning

IBM. (s.f.). *What are convolutional neural networks?* Recuperado de https://www.ibm.com/es-es/topics/convolutional-neural-networks

IBM. (s.f.). *Deep learning versus machine learning.* Recuperado de https://www.ibm.com/topics/artificial-intelligence

Jasper Susan (2022). *Cómo detectamos, eliminamos y denunciamos el material de abuso sexual infantil.* Recuperado de

https://blog.google/intl/es-es/productos/informacion/2022_10_como-detectamos-eliminamos-y/

Mathworks (s.f.). *Reconocimiento de imágenes con Machine Learning.* Recuperado de https://es.mathworks.com/discovery/image-recognition-matlab.html

Mathworks Inc. (s.f.). *Reconocimiento de imágenes con Deep Learning.* Recuperado de https://la.mathworks.com/campaigns/offers/next/machine-learning-vs-deep-learning.html

Mezmur, B. D. (2016). *Las directrices lingüísticas son una herramienta clave para abordar el abuso sexual infantil.* Organización de las Naciones Unidas. Recuperado de https://www.ohchr.org/en/press-releases/2016/06/language-guidelines-key-tool-tackling-child-sex-abuse-un-child-rights

Mi Argentina (2024). *Delitos informáticos en Argentina.* Jefatura de Gabinete de Ministros de la Nación. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-4

Microsoft (2009). *PhotoDNA* Recuperado de https://www.microsoft.com/en-us/photodna

Schneppat Jörg-Owe (2019). *Types of AI*. Schneppat AI. Recuperado de https://schneppat.com/types-of-ai.html

Yúbal Fernández. (2007). *Así era ELIZA, el primer bot conversacional de la historia.* Xataka. Recuperado de https://www.xataka.com/historia-tecnologica/asi-era-eliza-el-primer-bot-conversacional-de-la-historia

YouTube (s.f.). *Proteger a los menores en riesgo.* Recuperado de https://www.youtube.com/howyoutubeworks/our-commitments/fostering-child-safety/#protecting-minors-at-risk

Videos

Clearview AI (2022). *How Facial Recognition is Identifying Human Trafficking Victims.* Recuperado de https://www.youtube.com/watch?v=1G5hW1ZIHCg

Terre des Hommes (2014). SWEETIE - *Terre des hommes gegen Kinderprostitution.* Recuperado de https://www.youtube.com/watch?v=wObUgUlI4YU&list=PLx8n7ozHKB2yTgvXSnaX89JKUn9ks3mWg