UCES
UNIVERSIDAD DE CIENCIAS EMPRESARIALES Y SOCIALES

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

DERECHO A LA AUTODETERMINACIÓN INFORMATIVA E INTELIGENCIA ARTIFICIAL: INTERACCIÓN, PROBLEMÁTICAS Y CASOS REALES

Por Santiago Carlen[1] y Paula González[2]

Fecha de recepción: 14 de junio de 2022

Fecha de aceptación: 14 de junio de 2022

ARK CAICYT: http://id.caicyt.gov.ar/ark:/s23470151/13aqhk7xx

Resumen

El presente trabajo corresponde a la disertación pronunciada por Santiago Carlen en la III Jornada de Investigación en Derecho: desafiando barreras, activando propuestas, realizada en la Universidad de Ciencias Empresariales y Sociales (UCES) el 10 de junio de 2022 vía Zoom Institucional.

Se trata de una investigación en proceso desarrollada con Paula González, cuyo propósito es indagar el impacto que tiene el diseño y la implementación de

[1] Estudiante de Abogacía de la Universidad de Ciencias Empresariales y Sociales (UCES). Miembro del Instituto de Investigación en Formación Judicial y Derechos Humanos (UCES). Investigador de UCES en el Proyecto de Investigación “Los Derechos Humanos en Argentina ante los nuevos desafíos”, bajo la dirección de los Dres. Paola Urbina y Darío Spada. ORCID: https://orcid.org/0000-0002-5239-8714

[2] Abogada de la Universidad de Buenos Aires (UBA). Especialista en docencia universitaria por la Universidad Tecnológica Nacional (UTN). Doctoranda en Derecho de la Universidad de Ciencias Empresariales y Sociales (UCES). Docente en la carrera de Abogacía (UCES, sede San Francisco) y docente de nivel medio. Miembro del Instituto de Investigación en Formación Judicial y Derechos Humanos (UCES. Investigadora de UCES en el Proyecto de Investigación “Los Derechos Humanos en Argentina ante los nuevos desafíos”, bajo la dirección de los Dres. Paola Urbina y Darío Spada. ORCID: https://orcid.org/0000-0002-6858-2209

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

políticas públicas que utilizan Inteligencia Artificial (IA) en el ejercicio de derechos fundamentales, como el derecho a la intimidad y la autodeterminación informativa.

El trabajo plantea como hipótesis que el Estado argentino, comprendido tanto en su jurisdicción provincial como nacional, define políticas públicas que implementan IA sin prevenir ni medir el impacto en el goce de derechos fundamentales.

Se trata de una investigación no experimental, descriptiva, documental, básica, y de abordaje cuantitativo y cualitativo, modelo de esquema dominante, prevaleciendo lo cualitativo sobre lo cuantitativo.

Abstract

This work corresponds to the dissertation given by Santiago Carlen at the III Conference on Research in Law: challenging barriers, activating proposals, held at the University of Business and Social Sciences (UCES) on June 10, 2022 via Institutional Zoom.

This is an ongoing investigation, whose purpose is to investigate the impact of the design and implementation of public policies that use Artificial Intelligence (AI) in the exercise of fundamental rights, such as the right to privacy and informational self-determination.

The work hypothesizes that the Argentine State, included both in its provincial and national jurisdiction, defines public policies that implement AI without preventing or measuring the impact on the enjoyment of fundamental rights.

It is a non-experimental, descriptive, documentary, basic research, with a quantitative and qualitative approach, a dominant scheme model, with the qualitative prevailing over the quantitative.

UCES
UNIVERSIDAD DE CIENCIAS EMPRESARIALES Y SOCIALES

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Resumo

Este trabalho corresponde à dissertação proferida pelo Santiago Carlen no III Congresso de Pesquisa em Direito: desafiando barreiras, ativando propostas, realizado na Universidade de Ciências Empresariais e Sociais (UCES) em 10 de junho de 2022 via Zoom Institucional.

Esta é uma investigação em andamento, cujo objetivo é investigar o impacto do desenho e implementação de políticas públicas que utilizam Inteligência Artificial (IA) no exercício de direitos fundamentais, como o direito à privacidade e à autodeterminação informacional.

O trabalho levanta a hipótese de que o Estado argentino, incluído tanto em sua jurisdição provincial quanto nacional, define políticas públicas que implementam a IA sem prevenir ou medir o impacto no gozo dos direitos fundamentais.

Trata-se de uma pesquisa não experimental, descritiva, documental, básica, com abordagem quantitativa e qualitativa, modelo de esquema dominante, prevalecendo o qualitativo sobre o quantitativo.

Palabras claves

Inteligencia artificial, Políticas públicas, Derechos Humanos, derecho a la intimidad, derecho a la autodeterminación informativa.

Keywords

Artificial intelligence, Public Policies, Human Rights, right to privacy, right to informative self-determination.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

Palavras chave

Inteligência artificial, Políticas Públicas, Direitos Humanos, direito à privacidade, direito à autodeterminação informativa.

1. Consideraciones previas

Buenas tardes a todas y todos. En primer lugar, doy las gracias a las autoridades de la Universidad de Ciencias Empresariales y Sociales (UCES), a Paola Urbina y Darío Spada, a mis compañeras Paula González y Giselle Moreno y a todos los y las asistentes a este encuentro.

Hoy vamos a hablar sobre los avances que hemos podido concretar en el Proyecto de Investigación titulado “Derechos Humanos e Inteligencia Artificial. Panorama actual y desafíos en la República Argentina”.

La inteligencia artificial, en adelante (IA), irrumpe en el escenario global contemporáneo poniendo en tensión su implementación operativa con el goce y ejercicio de los derechos humanos fundamentales.

Con el propósito de continuar la problematización en dicha temática, en esta oportunidad nos preguntamos cuáles son los impactos que ocasiona el diseño e implementación de tecnologías que utilizan IA aplicadas a políticas públicas y proyectos privados respecto del goce y ejercicio de derechos fundamentales tales como la intimidad y la autodeterminación informativa.

Por supuesto, fueron ingentes las preguntas que nos surgieron a raíz del estudio del tema, cómo, ¿el desarrollo de IA requiere de una regulación concreta para evitar la vulneración de derechos fundamentales? ¿Una legislación que promueva el desarrollo de IA sostenible y legal es un límite suficiente para evitar lesiones a derechos fundamentales como el derecho a la privacidad y la autodeterminación? ¿La

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

modernización de los sistemas de control y vigilancia en nombre de la seguridad de la población, son sistemas seguros?

El presente trabajo constituye un nuevo avance correspondiente al Proyecto de Investigación “Los Derechos Humanos en Argentina ante los nuevos desafíos”, en particular, “Derechos Humanos e Inteligencia Artificial. Panorama actual y desafíos en la República Argentina”.

Con esta investigación nos proponemos indagar sobre cuál es el impacto que tiene el diseño y la implementación de políticas públicas que utilizan IA en el ejercicio de derechos fundamentales como el derecho a la intimidad y la autodeterminación informativa.

2. Hipótesis en proceso de demostración

En el trabajo nos planteamos como hipótesis a demostrar que el Estado argentino, comprendido tanto en su jurisdicción provincial como nacional, define políticas públicas que implementan IA sin prevenir ni medir el impacto en el goce de derechos fundamentales.

3. Metodología empleada

El presente trabajo es una investigación no experimental, de tipo descriptivo y documental, básica.

El abordaje de la investigación será cuantitativo y cualitativo, modelo de esquema dominante, prevaleciendo lo cualitativo sobre lo cuantitativo.

Analizaremos los documentos y normativa regulatoria de IA de nuestro país. Además, indagaremos sobre los datos obtenidos en base a experiencias de implementación de aplicaciones o programas diseñados con IA utilizadas en

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

Argentina, teniendo en consideración los criterios de selección para su uso, los alcances de los algoritmos utilizados y su impacto respecto del derecho a la intimidad y la protección de datos personales. De la misma manera, abrevaremos en la jurisprudencia nacional y extranjera.

Los instrumentos que utilizaremos son guías de pautas, cuestionarios y cuadros comparativos.

4. Derecho a la autodeterminación informativa

El patrón oro del mundo actual es la información.

Todos los días, regalamos fragmentos de datos personales sin pensarlo realmente. Lo hacemos cuando nos suscribimos a boletines, publicamos en las redes sociales o ingresamos nuestra información de contacto en un formulario. Lo hacemos porque confiamos en que las empresas a las que entregamos nuestros datos los usarán de manera responsable, para enviarnos anuncios dirigidos, recomendar contenido o asegurarse de que nuestra experiencia en sus sitios web sea lo más fluida posible. Pero ¿qué sucede cuando no lo hacen? ¿Qué sucede cuando venden nuestros datos a terceros? ¿O cuándo almacenan información privada que obtienen sin consultarnos, sobre nuestras conductas, consumos, sobre nuestro comportamiento en la red?

En las últimas décadas, vivimos una transformación de la forma de vida humana. La explosión de las tecnologías de la información y la comunicación, en adelante TICs, la globalización de internet, la introducción del *smartphone* en la cotidianeidad y la aparición de las redes sociales desdibujaron la barrera entre la esfera pública y la privada. Antes nuestra intimidad podía ser vulnerada a través de la toma de fotografías no consentidas (fallo Indalia Ponzetti de Balbín c/Editorial Atlántida S.A. s/ Daños y Perjuicios del año 1984), espionaje telefónico, el robo de

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

correspondencia privada o el *voyeurismo*. Hoy en día, con el uso masivo de internet y teléfonos inteligentes no solo es posible captar y transmitir información privada sin que los titulares se den cuenta, sino que además el hecho de acumular la máxima cantidad de información acerca de las personas se ha tornado un objetivo fundamental de la industria tecnológica y de los Estados.

La nueva configuración del tablero humano ha permitido ingentes lesiones a derechos fundamentales: abuso en el tratamiento de datos personales, robos de identidad, perfilamiento para la modificación de conductas, discriminaciones masivas, *grooming*, entre otros.

4.1 Concepto de autodeterminación informativa

Podemos comenzar a esbozar algunos puntos que versan en torno a lo que entendemos por derecho de autodeterminación informativa, el cual se encuentra íntimamente vinculado con el derecho a la intimidad, el honor y, en consecuencia, a la protección de los datos personales.

Es menester aclarar que, hasta la fecha, no se encuentra conceptualizado en nuestro ordenamiento jurídico, pero doctrinariamente se han esbozado ciertos lineamientos, tales como el que aporta Molina Quiroga (2003) al definirlo como la posibilidad que tiene el titular de los datos personales de controlar quienes serán destinatarios de dicha información y qué uso le darán, y al afirmar que se ejercita a través de los derechos de acceso, rectificación y cancelación.

De la misma manera, al estar indefectiblemente ligado al derecho a la intimidad y al honor, siendo ambos derechos personalísimos conforme su regulación en los arts. 18, 19, 33, 43 y 75 inc. 22 de la Constitución Nacional; arts. 52, 53 y 1770 del Código Civil y Comercial de la Nación.

La Corte Suprema de Justicia de la Nación ha sentado extensa doctrina acerca del derecho a la intimidad, a la cual adherimos:

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> ...el derecho a la intimidad y a la protección de la vida privada personal y familiar se halla garantizado por el art. 19 de la CN. Dicha norma otorga al individuo un ámbito de libertad en el cual este puede adoptar libremente las decisiones fundamentales acerca de su persona, sin interferencia alguna por parte del Estado o de los particulares, en tanto dichas decisiones no violen derechos de terceros. El derecho constitucional protege un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad. En rigor, el derecho a la privacidad comprende no solo la esfera doméstica, el círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas tales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello y solo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (CS, Fallos: 335:799). (“Denegri, Natalia Ruth C/ Google Inc. S/ Derechos Personalísimos: Acciones Relacionadas”, 2020).

El ejercicio de este derecho requiere mecanismos eficaces para que los titulares puedan: acceder a sus datos, controlar quién los tiene, saber quién puede utilizarlos y con qué fines, así como decidir en qué momento restringir o cancelar el uso de los mismos a terceros.

Siguiendo esta interpretación, el pilar sobre el que descansa la tutela de este derecho reside en el consentimiento informado que debe garantizarse al titular a la hora de proceder con el tratamiento de sus datos personales. En otras palabras, para el ejercicio pleno del derecho a la autodeterminación informativa debemos tener la certeza acerca de quién tiene nuestros datos y para qué los está usando, a los fines de consentir, corregir o cancelar la utilización y/o el contenido de los mismos.

Nuestros constituyentes plasmaron en la Constitución Nacional un pliego de derechos fundamentales inherentes a la persona humana, donde la intimidad, el honor

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

y la dignidad son primordiales. Protegieron estos derechos consagrando la inviolabilidad de la propiedad, el domicilio y la correspondencia privada sin orden escrita y fundada de autoridad pública (arts. 17 y 18 Constitución Nacional).

Esta especial tutela, que se completa mediante la incorporación del art. 43 en la reforma constitucional de 1994, donde se eleva a rango supremo el *hábeas data*, nos brinda una regla interpretativa que, para tornar operativa la Norma Fundamental, nos exige que el consentimiento informado sea requerido siempre en el tratamiento de los datos personales de una persona, ya que integran el bloque tutelado de propiedad privada, dignidad e intimidad y dado que lo contrario importaría una lesión a estas garantías.

Entonces, el derecho de autodeterminación informativa se unge como prerrogativa del individuo frente al Estado o particulares respecto de la recolección, conservación, tratamiento y transmisión de datos personales privados, por la cual nadie puede sin el consentimiento informado del titular siquiera acceder a ellos, sin importar si puede o no resultar en algún perjuicio. La forma de tornar operativa esta facultad es el procedimiento de *hábeas data.*

En el fallo “Cañadas Pérez, María Dolores c/Bank Boston S.A s/daños y perjuicios” del 2008, el Juzgado Nacional de Primera Instancia en lo Civil N° 39 sentó la siguiente doctrina al respecto:

> El derecho del particular forma parte de la vida privada, y se trata, como el honor y la propia imagen, de unos de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, su relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la llamada “autodeterminación informativa" (Considerando III, párr. 17).

Profundizando, podemos enumerar los caracteres que posee el derecho de autodeterminación informativa. Si bien la doctrina no es homogénea y existen diversas

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

caracterizaciones, describiremos nuestra propia caracterización. Por lo tanto, el derecho de autodeterminación informativa es:

- Inherente. El derecho nace con el sujeto, y su existencia es inseparable de su persona.
- *Erga omnes*. Oponible a todas las demás personas, sean públicas o privadas. Personalísimo. Solo el titular tiene legitimación para ejercerlo.
- Irrenunciable. Al ostentar calidad de derecho fundamental, no puede ser renunciado por el individuo.
- Imprescriptible. El tiempo no impide ni cancela el ejercicio del derecho.
- Extrapatrimonial. Si bien los datos que produce un individuo pueden ser considerados bienes, el derecho de autodeterminación informativa no trata sobre aspectos que sean susceptibles de apreciación económica. En otras palabras, no puede venderse ni comprarse el derecho, aunque sí los datos.

Autores como Noé Adolfo Riande Juárez (2022) agregan como caracteres: la cualidad de “derecho subjetivo privado”, ya que garantiza el goce de las facultades del individuo; la condición de “variable”, en tanto su contenido depende de las circunstancias en las cuales se desarrolla y su origen “interno”, debido a su procedencia particular y de conciencia (p. 8).

Por su parte, el Código Civil y Comercial de la Nación, aprobado por ley N° 26.994, hace referencia expresa a los derechos personalísimos, estableciendo que “La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos…” (art. 52). Y de igual forma, en su art. 53 exige que “…para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento”.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

Sin embargo, y en consonancia con las reglas interpretativas constitucionales, los derechos no son absolutos y existen excepciones que habilitan ciertas limitaciones o restricciones en el ejercicio. Un ejemplo de esta relatividad en cuanto a la autodeterminación informativa la encontramos en el Registro Provincial de Perfiles de ADN de la provincia de Córdoba, donde se realiza un registro genético de los condenados por delitos contra la integridad sexual sin su consentimiento ni capacidad de modificar esta situación.

En tal sentido, el Tribunal Superior de la provincia de Córdoba, ante el pedido de inconstitucionalidad de las leyes 9.680 y 9.864, que crean y establecen el régimen del Registro antes mencionado, decidió que la restricción al derecho a la intimidad y autodeterminación informativa era válida, pues proviene de una ley, la cual persigue un fin legítimo y cumple con los requisitos de idoneidad, necesidad y proporcionalidad. (C.L.A S/ Ejecución de pena privativa de la libertad - Recurso de Inconstitucionalidad, 2015).

Siguiendo este punto, la ley de protección de los datos personales, en adelante LPDP, en su art. 5°, inciso 2, detalla en qué casos no será necesario el consentimiento informado para el tratamiento de datos personales, y establece la excepción cuando:

> a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. (LPDP).

4.2 Datos personales

La ley 25.326 de Protección de Datos Personales, en adelante LPDP, define a los mismos en su art. 2° como:

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". A su vez, delimita a aquellos datos que son "sensibles", en tanto revelen "origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Los considerados datos sensibles gozan de protección especial según los arts. 7° y 8° de la LPDP, los cuales establecen, por una parte, que no hay obligación de proporcionar datos sensibles y, por otra, que el tratamiento de estos datos sólo puede hacerse si media interés general autorizado por ley o si su tratamiento es con fines científicos y estadísticos, con la debida precaución de que los titulares no puedan ser identificados.

Asimismo, es necesario traer a colación el art. 53 del Código Civil y Comercial de la Nación, que tutela el derecho a la imagen, prescribiendo que …"para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento…", tras lo que puntualiza tres excepciones: a) cuando la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario y se procure no dañar innecesariamente a nadie y, c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

Los datos, a su vez, deben ser considerados bienes particulares, en tanto son de uso común, son susceptibles tanto de apreciación económica como de apropiación y no son de dominio originario del Estado (art. 238 del Código Civil y Comercial de la Nación).

Tal como sostiene Riande Juárez (2022), el paso de la información privada de una persona desde la esfera íntima a la esfera social transforma un atributo de la personalidad, intimidad e identidad en un bien jurídico, dato personal, que el Estado debe proteger, regular y vigilar, en cuanto es el encargado de mantener el orden social y preservar el imperio de la Constitución (p. 7).

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

> El art. 1° de la LPDP circunscribe el objeto a tutelar de la siguiente manera
>
> Los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
> Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
> En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

Al respecto cabe realizar dos consideraciones. En primer lugar, nos resulta poco abarcativa de la realidad la inclusión de los bancos de datos privados con el requisito especial de que deben estar destinados a dar informes.

Nos preguntamos qué sucede entonces con el uso de datos personales por particulares para definir y crear perfiles de consumidores/as y/o votantes. ¿Cuál es la extensión del concepto “informes”? Por otro lado, se observa una contradicción al otorgar a las personas jurídicas legitimación para ejercer este derecho (art. 1°, segundo párrafo), ya que, según los estándares internacionales en la materia, las personas de existencia ideal no son sujetos titulares de derechos humanos fundamentales.

En nuestro país, la autoridad encargada del control de la LPDP es la Dirección Nacional de Protección de Datos Personales (DNPDP). Esta dependencia tiene la potestad de sancionar las violaciones a la ley.

Asimismo, en virtud del fuerte crecimiento de la industria del *software*, en el año 2015 se aprobó, por Disposición 18/2015 de la Dirección Nacional de Protección de Datos Personales, la denominada “Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones” en la cual se reconoce que “...una gran parte de los tratamientos de datos personales se llevan a cabo mediante aplicaciones de

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

programas de software, en muchos casos de manera automática o con escasa supervisión de una persona".

Esta guía representa un documento orientativo con pautas de conducta en relación a la protección de datos personales y a la aplicación de políticas de privacidad en el campo del desarrollo de aplicaciones, estableciéndose qué tratamiento de datos personales, automatizados o no, deben ser diseñados y desarrollados de manera que respeten los principios y las obligaciones legales, debiendo contemplarse debidamente el resguardo de la privacidad de los titulares de la información personal tratada (Anexo I, Disposición 18/2015 DNPDA).

4.3 Marco jurídico: plexo normativo de nuestro ordenamiento argentino y tratados internacionales de derechos humanos

Es menester mencionar las herramientas jurídicas que el orden normativo argentino contempla actualmente respecto a la tutela del derecho de autodeterminación informativa y para ello, los arts. 18, 19, 33, 43 y 75 inc. 22 de la Constitución Nacional resultan fundamentales.

El derecho a la intimidad está ampliamente cubierto por los preceptos de la Carta Magna, lo que engloba la autodeterminación informativa a través de la inviolabilidad de los papeles privados (art. 18), las acciones privadas y el principio de legalidad (art. 19), los derechos implícitos (aquí estaría la autodeterminación informativa específicamente) -art. 33-, el habeas data (art. 43) y el orden tuitivo internacional contemplado en la Declaración Universal de los Derechos Humanos (1948), el Pacto Internacional de Derechos Civiles y Políticos de la ONU (1966), el Pacto Internacional de Derechos Económicos, Sociales y Culturales y el Pacto de San José de Costa Rica (art. 75 inc. 22).

Asimismo, el art. 12 de la Declaración Universal de los Derechos Humanos, establece que el derecho a la vida privada es un derecho humano, y que "Nadie será

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En la misma línea el art. 17 del Pacto Internacional de Derecho Civiles y Políticos consagra, al respecto, lo siguiente:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Por su parte, el art. 11 de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) establece una norma de protección a la honra y la dignidad, al prescribir:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Como refiriéramos anteriormente, la ley 25.326 de Protección de Datos Personales y su decreto reglamentario 1558/2001 son las normativas específicas donde de manera más comprensiva y concreta se protegen los datos personales, contemplando la recolección del dato, el tratamiento o procesamiento, la comunicación e información que se haga a terceros de estos y la cesión de los mismos, así como los principios que rigen al respecto: principio de calidad de los datos, principio de información, principio de consentimiento y principio de seguridad.

En la Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones, que antes mencionáramos, creada por la disposición 18/2015 de la Dirección Nacional de Protección de Datos Personales, se introducen conceptos como "privacidad desde el diseño" y "privacidad por defecto". El primero de ellos, se refiere

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

a que desde el origen mismo del diseño de un sistema, aplicación o dispositivo se debe contemplar la protección de la privacidad de los datos personales en todas las etapas del ciclo de vida del sistema, aplicación o dispositivo. El concepto de privacidad por defecto implica que la configuración de la privacidad debe estar activada de forma predeterminada, siendo un acto de voluntad del titular desactivar o compartir información personal.

Además, debemos mencionar la ley 26.522 de Servicios de Comunicación Audiovisual y su decreto reglamentario 1225/2010, los cuales estatuyen que la sociedad de la información debe basarse en valores aceptados universalmente, promover el bien común e impedir la utilización indebida de las TIC, así como proteger la privacidad y los datos personales (art. 25, inc. c).

Por último, mencionamos en el listado de normativas vigentes la ley 26.529 de derechos del paciente en su relación con los profesionales e instituciones de salud y su decreto reglamentario 1089/12, donde se contempla una especial protección de los datos sensibles médicos (art. 2°, inc. c); la ley 27.078 -Argentina Digital-, específicamente los arts. 5° y 59° inc. f y, por último, la ley 27.275 de Derecho de Acceso a la Información Pública y su decreto reglamentario 206/2017, donde se contempla la excepción a proveer información al solicitante cuando se trate de datos personales y no pueda brindarse aplicando procedimientos de disociación (arts. 8° inc. i y 34).

5. Inteligencia artificial

5.1 Concepto

La IA, irrumpe en el escenario global contemporáneo poniendo en tensión su implementación con el goce de los derechos humanos fundamentales. Desde sus orígenes ha dado nacimiento a múltiples teorías y métodos de abordaje acerca de

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

esta temática tan compleja. No existe acuerdo académico acerca de su definición, por lo que es un concepto multívoco.

A nivel general, podríamos definir a la IA como una "…revolución de la escritura, montada sobre la electricidad, internet, algoritmos y computadoras" (Corvalán, 2021, p. 11). El objetivo principal de este constructo humano no es otro que el de hacer más sencilla la vida, como toda la tecnología creada desde los orígenes.

Así como las herramientas manuales nos hicieron más fácil la tarea de recolectar y construir, las armas nos han facilitado la tarea de defendernos o atacar y la ropa nos ha permitido más sencillamente mantener el calor y evitar las heridas, la IA viene a hacernos más simple la tarea de pensar, analizar y tomar decisiones.

Para el desarrollo del presente trabajo, tomaremos la definición brindada por la Comisión Europea, la cual afirma que "El término «inteligencia artificial» (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía- con el fin de alcanzar objetivos específicos" (Cotino Hueso, 2019, p. 3). A esta definición podría agregarse que el entorno que es capaz de analizar la IA puede ser tanto físico como digital, o ambos.

Es importante destacar que el nodo que conecta lo que entendemos por inteligencia humana con IA es simplemente la capacidad de reconocer patrones de información y actuar en consecuencia. Es inconcebible, por ahora, que la IA pueda replicar perfectamente la mente humana, tan solo podrá reproducir el aspecto resolutivo que actúa a través de la cognición. En este sentido, lo mismo aplica inversamente, la inteligencia humana no puede ni podrá replicar a la perfección la forma de intelecto de las máquinas.

Sin embargo, es menester tener en cuenta que el proceso de evolución y aprendizaje de la IA funciona radicalmente distinto al del cerebro humano.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Sostiene Kurzweill (2013) que nuestro intelecto evoluciona de manera aritmética, es decir, linealmente y de a un "escalón", mientras que la IA evoluciona y aprende de manera exponencial, es decir, que su crecimiento es proporcional a su valor actual, o, en otras palabras, si midiéramos la evolución en escalones, y la IA comienza en el escalón dos, su siguiente escalón no será el tres, sino el cuatro, y el siguiente será el ocho, y así sucesivamente. Lo que un ser humano tarda treinta escalones en alcanzar, una IA lo alcanzaría en apenas cinco y cada salto la aleja vertiginosamente del anterior.

Además, cabe agregar la problematización que hacen al respecto expertos en la materia tales como Corvalán, Díaz Dávila y Simari (2021), quienes expresan la posibilidad de concebir una IA débil frente a una conceptualización de IA fuerte.

En ese sentido los autores afirman que:

> Se llama IA "débil", "restringida", "estrecha" o "blanda" al procesamiento de datos e información para resolver problemas y tomar decisiones a partir de utilizar algoritmos inteligentes, sobre la base de aplicar diferentes técnicas informáticas. La idea básica, en esta conceptualización, es obtener resultados específicos en ciertas actividades o ámbitos concretos que antes solo podían obtenerse a partir de nuestros cerebros, idónea para un problema en un dominio definido a priori (p. 27).

Por su parte, la IA fuerte implicaría para algunos la posibilidad de una máquina con capacidad para replicar completamente la función del cerebro humano en cada uno de sus aspectos (Warwick, p. 25), en una visión más cercana a la de Alan Turing, quién desarrolló en 1950 el famoso "juego de la imitación", posteriormente reconocido como "test de Turing", donde se planteaba que un sistema informático era inteligente si podía hacerse pasar por un ser humano en una conversación por texto con otra persona, sin que la misma se dé cuenta de que está hablando con una máquina.

Para otros, en cambio, el nacimiento de una IA fuerte implicaría un riesgo para toda la humanidad, ya que este tipo de inteligencia no solo sería capaz de copiar la mente humana, sino que tendría, a su vez, la potencia de las máquinas, a saber:

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

capacidad de almacenamiento de información ilimitadamente extensible, velocidad de procesamiento infinitamente mayor a cualquier ser vivo y capacidad de conexión con otros sistemas de forma instantánea.

Así, Kaku (2013) plantea que si una IA lograra por un lado replicar la inteligencia humana, es decir, sentido común, capacidad de sentir, de reconocer el entorno y a sí mismo, y por otro, desarrollar una "inteligencia general", capaz de aprender de cualquier eventualidad, se produciría una "explosión de inteligencia", ya que la máquina poseería un conocimiento exponencialmente más profundo que el de cualquier ser humano, podría iniciar un ciclo de automejora y de "autoconsciencia", y a su vez, construir otras máquinas conscientes y cada vez mejores (pp. 142-144).

Elon Musk (2018), uno de los empresarios *tech* de IA más importantes del mundo, advierte del peligro de la IA, y afirma que "*es mucho más peligrosa que las armas nucleares*".

Sentado esto, cabe destacar que en la actualidad solo convivimos con IAs débiles, que no son otra cosa que algoritmos de automatización. Es una tendencia común asociar IA a robots postapocalípticos, pero nada nuevo realmente irrumpe en la vida cotidiana del ser humano, ya que hace siglos que utilizamos algoritmos, la única diferencia es que ahora son mucho más complejos.

Actualmente, por defecto, consideramos que cuestiones simples como apretar un botón en el celular y que unos días después nos llegue lo que encargamos a nuestra casa no tiene nada que ver con IA, pero en esta concepción débil, que para cualquier ser humano nacido antes de 1900 parecería prácticamente brujería, no vemos más que tecnología naturalizada, sucede así que "tendemos a considerar "no inteligentes" tareas que se vuelven sencillas y habituales con el paso del tiempo" (Corvalán, Díaz Dávila y Simari 2021, p. 25).

Estamos rodeados de algoritmos y, por lo tanto, de IA.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Los algoritmos son conjuntos de reglas utilizados para resolver problemas y tomar decisiones, autores como Benítez, Escudero, Kanaan, y Masip Rodó (2013) acuerdan en esta definición, aunque también cabe la conceptualización de los mismos como "...códigos informáticos diseñados y escritos por seres humanos que ejecutan instrucciones para traducir datos en conclusiones, información o productos..." (ONU, 2020).

Un ejemplo de algoritmo básico es una receta de cocina o una lista de instrucciones para armar un mueble. En cambio, un algoritmo de IA es entrenado para convertirse en un agente inteligente (Rusell & Norvig, 2016), es decir, en un sistema parcial o totalmente autónomo, capaz de aprender, reconocer su entorno, actuar en consecuencia e incorporar sus experiencias a su base de conocimiento para transformarlas en un vector de evolución.

5.2 Aprendizaje automático (*machine learning*), aprendizaje profundo (*deep learning*) y redes neuronales

El aprendizaje automático, someramente, se trata del sistema de aprendizaje programado en un algoritmo que, en un primer momento, construye representaciones de los datos a los que accede, moldea una base de conocimiento, desarrolla una lógica de razonamiento y define un modelo de aprendizaje, todo con el objetivo de ser capaz de reconocer su entorno, entendido como el espacio físico o digital donde vaya a ejecutarse, y actuar en consecuencia de los objetivos que tenga programados.

Una vez logrado esto, el algoritmo se transforma en un agente inteligente capaz de actuar de manera autónoma, aprender de su propia experiencia y desarrollar nuevas soluciones a las variables que se le presenten.

El *machine learning* abarca a todas las tecnologías que aprenden a través del entrenamiento con bases de datos y donde es posible auditar cada paso y decisión

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

tomada por el algoritmo y que usualmente son denominados algoritmos de “caja blanca”.

Por su parte, el *deep learning* está asociado a las IAs denominadas “redes neuronales”, que tienen una particular forma de funcionamiento, caracterizado por la opacidad de su programación. Por ello los sistemas que utilizan este proceso son denominados como algoritmos de “caja negra”, donde no es posible observar las decisiones del algoritmo utilizadas para resolver un problema en concreto. Además, requieren ingentes cantidades de datos -*big data*- para su entrenamiento (OCDE, 2019).

Lo que hace, básicamente, un sistema de redes neuronales artificiales es imitar el funcionamiento del cerebro humano. Así como las neuronas reaccionan ante estímulos y se activan transmitiendo la conclusión realizada en base al estímulo captado a todas las neuronas a las que está conectada, las redes neuronales artificiales hacen lo mismo, o lo intentan.

Pueden clasificarse en dos grandes grupos: sistemas supervisados y sistemas no supervisados. Los primeros tienen una guía que los va conduciendo, los segundos aprenden por sí mismos los patrones que encierran los datos (Corvalán, Díaz Dávila y Simari, 2021, p. 48).

Un ejemplo icónico de ambos tipos de sistemas lo podemos encontrar en los proyectos “*Alpha Go*” y “*Alpha Go Zero*” de *Google Mind*. El primero es un sistema supervisado con una base de datos de la cual aprender, y que fue capaz de derrotar a más de sesenta jugadores expertos humanos en distintos juegos, principalmente en el juego “Go” que le dio su nombre. El segundo es un sistema no supervisado, sin una base de datos de aprendizaje, es decir, aprendió desde cero a jugar contra él mismo, y en apenas tres días, después de casi cinco millones de partidas jugadas pudo derrotar a su versión previa.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Los principales usos que se le dan a este tipo de IAs, que utilizan *machine learning* o *deep learning*, son: la automatización de tareas, la elaboración de predicciones, detección inteligente de patrones complejos y ejecución de soluciones que tradicionalmente tendrían un alto costo o resultan imposibles de realizar a un ser humano.

5.3 *Big data* o macrodatos: el alimento de la IA

"Cada tres años se genera un volumen de datos que representa al que se produjo en la historia de la humanidad. El flujo de información es el oxígeno de la inteligencia artificial que, a su vez, ésta retroalimenta" (Corvalán, 2021, p. 9).

Es importante comprender que la IA se "alimenta" de datos, los necesita como el ser humano requiere de estímulos para aprender. Sin embargo, un dato de manera aislada no tiene gran valor, es necesaria la conjunción de datos (*dataset*) para que el algoritmo pueda procesarlos y aprender. A su vez, este conjunto de datos debe presentar una consistencia y plenitud que permita una organización adecuada y lógica ya que, de lo contrario, el algoritmo no podría distinguir entre la información verdadera y la falsa. En otras palabras, si en el *dataset* de la IA existe un dato replicado con dos resultados diferentes (ej. x = 2; x = 3), o existen lagunas y huecos de información, el producto que surja del algoritmo estará sesgado.

Ocurre que las IAs que utilizan aprendizaje profundo en conjunción con un sistema de redes neuronales artificiales para funcionar correctamente requieren procesar millones de datos interrelacionados en busca de patrones de estimulación que disparen una neuro respuesta artificial, en función del proceso de construcción y evolución del algoritmo. Es decir, para brindar una respuesta ante determinada pregunta hecha al sistema, indagará en sus *datasets*, seleccionará la información a producir en base a un criterio subsimbólico, aprendizajes propios de la IA y objetivos

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

programados, generará una sinapsis artificial que pondere entre todas las capas de neuronas la información obtenida y brindará un resultado o conclusión razonada.

Podemos ilustrar esto con un ejemplo: si buscamos en el motor de búsqueda de Google imágenes de autos, el algoritmo tendrá que analizar las millones y millones de imágenes con etiquetas asociadas al concepto de auto, discriminar las que les resulten más estimulantes y brindar un resultado ponderado al usuario/a.

Sin embargo, pueden existir errores en el criterio de ponderación y selección de información, originados por los conocidos "caballos de Troya" y los sesgos algorítmicos, conceptos sobre los que volveremos seguidamente.

Si se proporciona suficiente cantidad de información etiquetada de forma incorrecta, ambigua o sesgada al algoritmo, éste no podrá distinguir correctamente los patrones y brindará respuestas defectuosas.

Es menester, antes de continuar, esbozar una breve definición de "sesgo algorítmico". Cómo define Sánchez Caparrós (2021), el sesgo es "...aquella inclinación (como prejuicio o estereotipo) que perjudica a una persona o grupo de personas, sea directa o indirectamente, dando lugar a resultados discriminatorios" (p. 306).

Utilicemos otro ejemplo para ilustrar este importante concepto: imaginemos que una empresa X solicita a un programador que diseñe una IA para que realice las búsquedas de personal y seleccione a los mejores candidatos. El programador deberá entrenar al algoritmo con información y preguntarle a la empresa cuál es su criterio acerca de lo que es un mejor candidato. La empresa proveerá al programador con toda la información histórica de la empresa, que tiene más de cuarenta años de trayectoria, indicando quiénes fueron sus mejores empleados, los más exitosos y que más dinero ahorraron e hicieron ganar a la empresa. El programador cargará todos estos datos, pondrá a entrenar al algoritmo y, una vez listo, lo presentará a la empresa, que inmediatamente lo pondrá en funcionamiento. Aquí comienza el problema, ya que, en los últimos cuarenta años y en el contexto socio-cultural que imperó durante toda

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

la trayectoria de la empresa, los únicos candidatos exitosos de la empresa fueron hombres caucásicos, formados en las universidades más caras, de clase alta y heterosexuales. La IA no tiene la capacidad de darse cuenta de que seleccionar solo a estos candidatos es un acto discriminatorio y, en base a su programación y sus *datasets*, reproducirá esta discriminación *ad infinitum.*

Esto es lo que se conoce como un algoritmo sesgado, que podrá serlo por defectos de programación, es decir, traslación ideológica del programador o de la base de datos al programa, o por acción de un tercero que busque infectar la IA para sesgarla a propósito, lo que denominamos caballo de Troya.

En palabras de Corvalán, Díaz Dávila y Simari (2021):

> Si la muestra de datos presenta patrones de discriminación social, la red, de comportarse como se espera, los reproducirá y puede que, hasta los amplifique, ya que su capacidad de aprendizaje, a través de la evolución de sus pesos sinápticos, es altísimo (p. 52).

6. Políticas públicas: conceptualización

A continuación, esbozaremos una somera definición de lo que entendemos por política pública, en los términos que plantearon Oszlak y O'Donnell (1976), al expresar que: "...las políticas estatales permiten una visión del Estado "en acción", desagregado y descongelado como estructura global y "puesto" en un proceso social en el que se entrecruza complejamente con otras fuerzas sociales" (p. 5).

Es decir, las políticas públicas implican el posicionamiento del Estado acerca de una cuestión socialmente problematizada, donde intervienen una multiplicidad de actores.

No todas las demandas o necesidades de la población son atendidas a través de una acción del Estado. Solo aquellas que alcanzan cierto rango socialmente

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

relevante pasan a ser objeto de enfoque por diversos grupos, organizaciones y el Estado mismo a fin de resolverla, priorizando ciertos intereses.

Ante una situación problematizada socialmente que adquiere relevancia, el Estado puede intervenir por acción o por omisión, pero en ambos casos estará tomando una decisión acerca de a quién va a privilegiar su postura.

En síntesis, las políticas públicas son:

> …un conjunto de acciones y omisiones que manifiestan una determinada modalidad de intervención del Estado en relación con una cuestión que concita la atención, interés o movilización de otros actores en la sociedad civil. De dicha intervención puede inferirse una cierta direccionalidad, una determinada orientación normativa, que previsiblemente afectará el futuro curso del proceso social hasta entonces desarrollado en torno a la cuestión (Oszlak & O'Donnell, 1976, p. 14).

7. ¿Cómo impacta el uso de IA en el ejercicio del derecho de autodeterminación informativa?

Consideremos que los riesgos que implica la utilización de IAs en el efectivo ejercicio y goce del derecho de autodeterminación informativa son enormes, ya que, en primer lugar, las IAs requieren grandes bases de datos para alimentarse y poder funcionar correctamente.

Un claro ejemplo de esto queda ilustrado en las IAs aplicadas al comercio, perfilamiento de potenciales clientes/votantes, *microtargeting,* modelación de redes sociales adaptadas al usuario/a, atención al público y en general, a toda actividad donde el algoritmo deba aprender a predecir el comportamiento humano para producir resultados, donde es necesario que consuma ingentes cantidades de datos personales.

Esto implica que, para la efectiva tutela del derecho a la autodeterminación informativa, los ordenamientos jurídicos deberán prever mecanismos donde los titulares de los datos sepan y acepten que su información será utilizada para entrenar

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

y desarrollar una IA, y que en cualquier momento puedan desistir y cancelar el uso de sus datos.

Frente a este escenario, es muy diferente el enfoque que se adopta de cara a estas técnicas cuando se trata de implementarlas en el Estado. En el sector público las decisiones y acciones deben justificarse, motivarse o explicarse.

Es crítico describir los procesos asociados a la toma de decisiones que importan al bien común y, por ello, es indispensable explicar íntegramente la correlación entre los datos, su procesamiento y los resultados.

Sin embargo, por el momento no resulta una tarea sencilla ni puesta en práctica, así nos lo refieren Corvalán, Díaz Dávila y Simari (2021)

> Por lo tanto, al menos por ahora, no es posible determinar por completo el paso a paso de la lógica del procesamiento de datos que sucede en el interior un sistema basado en deep learning (aprendizaje profundo), es decir, lo que pasa en las capas ocultas de la red. Y esto, en términos jurídicos, impide que el propio sistema o las personas puedan desarrollar una motivación, fundamentación o explicabilidad en cuanto a los resultados obtenidos (p. 63).

Particularmente creemos que existen enormes dificultades para realizar esto, teniendo en cuenta como se manejan las grandes corporaciones de datos y de tecnología. A modo de ejemplo citamos el caso de *Cambridge Analytica*, quienes no detendrán el avance y la producción de IAs, aunque esto implique la violación de la autodeterminación informativa de los titulares de los datos, al menos que se lleve luz a sus talleres de desarrollo de algoritmos, programación, y a las bases de datos utilizadas para el entrenamiento.

En segundo lugar, la IA es condición necesaria para el análisis del *big data*, lo que implica grandes riesgos, también, para los titulares de datos. Coincidimos con Gil (2016) sobre el riesgo de caer en conclusiones erróneas que nadie revisa; también el peligro que para las personas pueda tener tomar decisiones automatizadas con un sesgo humano; y, por último, la inseguridad para la privacidad de las personas (p. 32).

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

La aparición de mega corporaciones vinculadas a las nuevas tecnologías (*big tech*) enmarcadas en el crecimiento exponencial de la globalización transforma el escenario político, económico y social a nivel global, ya que traspasan fronteras con una profundidad nunca antes lograda por una empresa privada y cuentan con un poder tecnológico y monetario sin precedentes. No hay más que mirar cómo han crecido las corporaciones tecnológicas en los últimos veinte años logrando desplazar a empresas con siglos de existencia y desarrollo.

Estas *big tech* recaban datos de manera masiva (*Google, Meta, Apple*, *Amazon*, MercadoLibre) a fin de alimentar a sus algoritmos y producir riqueza. La aparición de las redes sociales ha transformado completamente la forma de relacionarse, buscar empleo, comunicarse y, fundamentalmente, de consumir de la población. Vemos cómo el concepto de intimidad se ve desdibujado en las nuevas generaciones y no sabremos las consecuencias que ello traerá a la *psiquis* humana.

Lo que sí podemos observar y coincidimos con Vercelli (2021), son los ostensibles beneficios que han traído consigo estas nuevas tecnologías, así como la profundización de injusticias socioeconómicas, las asimetrías jurídico-políticas y la atomización creciente de los tejidos de solidaridad social.

Es imperante que nos aboquemos al abordaje de la problemática que la IA plantea en el campo jurídico a fin de lograr extraer los beneficios que implica, disminuir los riesgos y lograr soluciones eficaces que traigan más justicia y equidad al sistema democrático.

8. Privacidad: datos personales

Las filtraciones de datos personales sensibles o de información industrial o estatal están a la orden del día. Errores en la ciberseguridad de los bancos de datos o de los dispositivos que tratan información sensible y privada han generado múltiples

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

casos a nivel mundial donde los derechos de miles o millones de personas fueron vulnerados. Desde el renombrado caso de *Cambridge Analytica* donde se manipuló a millones de votantes estadounidenses hasta los típicos casos de robo de identidad (*pishing*), la sociedad de la información contemporánea convive diariamente con vulneraciones a su intimidad y a su autodeterminación informativa por la mano de algoritmos sin siquiera saberlo.

Vivimos en la era de la información y cada cosa que hacemos o no hacemos es tenida en cuenta por las IAs puestas al servicio del mercado.

Cada una de nuestras decisiones y omisiones está contribuyendo a construir una identidad digital, observada por algoritmos de IA que modelan los estímulos que nos llegarán a través de la tecnología. Desde cuánto tiempo pasamos frente a una pantalla, viendo un contenido en particular, hasta cuánto tardamos cotidianamente en ir y volver del trabajo.

Existen infinitas potencialidades para esta revolucionaria tecnología, sin embargo, el resultado de la construcción de perfiles a los fines de predecir nuestro comportamiento y modificarlo obedece en general a intereses comerciales y/o privados transnacionales, lo que plantea serios problemas a nivel jurídico, a saber: límites a la libertad de expresión ilícitos, ingeniería conductual sobre la población, discriminaciones, violaciones a la intimidad, identidad y propiedad, y un largo etcétera.

Es de público y notorio conocimiento general que la enorme mayoría de usuarios de internet no lee los extensos términos y condiciones que imponen las *big tech* para permitirnos usar sus servicios.

Asimismo, es importante aclarar que ni Google, ni Netflix, ni Spotify, ni Meta y su constelación de aplicaciones son gratuitas. Nos cobran en el petróleo de nuestro siglo: los datos. La información que obtienen es tan valiosa que en pocos años pasaron a competir en poder y riqueza con multinacionales, magnates de la industria y los mismísimos Estados Nacionales.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

Los usuarios, en general, desconocen las consecuencias que tiene sobre su persona y sobre la sociedad el uso cotidiano de las redes sociales, más allá del hecho de que muchos de los términos y condiciones sean groseramente inconstitucionales, a lo que nos referiremos más adelante.

Para mayor ahondamiento, es recomendable ver los documentales “Nada es privado” y “El dilema de las redes sociales”.

Las personas usuarias deben otorgar su consentimiento informado, libre y expreso, como ya comentamos anteriormente, para el tratamiento de sus datos personales, de acuerdo al art. 5° de la LPDP, pero, como informa la Organización de Consumidores y Usuarios (2018) ¿Qué ocurre cuando nueve de cada diez usuarios no leen los contratos a los que se someten? ¿Puede interpretarse que existe consentimiento informado si uno de los contratantes no sabe siquiera que está consintiendo?

9. Extractivismo masivo de datos: el fenómeno de las *Big Tech*

Para hablar sobre el uso de datos personales por parte de las empresas de tecnología, quienes son las dueñas de motores de búsquedas, de redes sociales, nos resulta convincente lo que escribe al respecto Zuboff (2021). En su último libro, llamado “La era del Capitalismo de la Vigilancia”, aborda de manera descriptiva y elocuente sobre la intimidad de los usuarios frente a internet, en su sentido más abarcativo y también sobre el uso de los datos personales de los usuarios que están en poder de las empresas. Además, plantea categorías conceptuales que iremos desarrollando en estas líneas.

Como puntapié a este tema, tomaremos las conceptualizaciones que hace la autora citada del capitalismo de la vigilancia, quien lo define de la siguiente manera:

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

> 1. Nuevo orden económico que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales ocultas de extracción, predicción y ventas. 2. Lógica económica parasítica en la que la producción de bienes y servicios se subordina a una nueva arquitectura global de modificación conductual. 3. Mutación inescrupulosa del capitalismo caracterizada por grandes concentraciones de riqueza, conocimiento y poder que no tienen precedente en la historia humana. 4. El marco fundamental de una economía de la vigilancia. 5. Amenaza tan importante para la naturaleza humana en el siglo XXI como lo fue el capitalismo industrial para el mundo natural de los siglos XIX y XX. 6. Origen de un nuevo poder instrumentario que impone su dominio sobre la sociedad y plantea alarmantes contradicciones para la democracia de mercado. 7. Movimiento que aspira a imponer un nuevo orden colectivo basado en la certeza absoluta. 8. Expropiación de derechos humanos cruciales que perfectamente puede considerarse como un golpe desde arriba: un derrocamiento de la soberanía del pueblo (Zuboff, 2021, “Definición”, párr. 1).

A los fines de nuestro trabajo de investigación nos parecen importantes las acepciones al término capitalismo de la vigilancia número 1 y número 8.

Este concepto del capitalismo de la vigilancia nos resulta claro para mirar con atención lo que sucede a diario con la información a la que accedemos, producimos, compartimos.

Sostiene la autora, que el capitalismo de la vigilancia tiene el foco en el comportamiento humano como su materia prima, comportamiento humano al que la autora denomina “excedente conductual”. Esta materia prima es obtenida de manera gratuita, con un claro propósito: se conocen las conductas -gustos, preferencias, ideas, orientaciones sexuales, orientaciones políticas y más- para con ello fabricar productos predictivos que prevén los que los usuarios hacen y harán.

Los productos predictivos se convierten en insumos con información altamente negociable y con mucho valor para los adquirentes tales como publicistas o empresas proveedoras de servicios o de bienes.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Una de las empresas que más desarrolló esta tecnología de la predicción con la información obtenida por los usuarios, es Google, sostiene Zuboff (2021) que "Google se convirtió en la pionera, la descubridora, la elaboradora, la experimentadora, la principal practicante, el modelo y el foco difusor del capitalismo de la vigilancia" (p. 92).

El capitalismo de la vigilancia está definido por dos etapas bien precisas: en un primer momento, la extracción de datos los que, analizados, darán un producto de predicción como resultado del uso de tecnología del aprendizaje de las máquinas, *machine learning* y *deep learning*, configurando el segundo momento.

Como vemos, son los usuarios quienes producen datos, la materia prima del proceso del capitalismo de la vigilancia. El producto consiste en predecir las conductas, y es el objeto más preciado y vendible a las empresas, quienes son los clientes de Google*,* por ejemplo, así lo resalta Zuboff (2021):

> La publicidad siempre había sido un juego adivinatorio: una cuestión de arte; relaciones, opiniones y prácticas establecidas, pero nunca una "ciencia". La idea de poder trasladar un mensaje particular a una persona en concreto justo en el momento en que más probabilidades tendría de influir realmente en su comportamiento era- y siempre ha sido- el santo grial de la publicidad (p.112).

Y aquí, Google se lució, ya no tomaría datos de los usuarios para mejorar el servicio para ellos, sino que comenzaría a implementar la conocida "minería de datos", el llamado extractivismo, que tiene otro blanco, para nada vinculado a la mejora del servicio hacia los usuarios. En orden de lograr el fin de predecir comportamientos para vender de manera precisa un producto o un servicio, deberán analizar los datos, el comportamiento de miles, millones de usuarios, para que reciban anuncios publicitarios acordes y dirigidos a los intereses que demostraron durante sus interacciones con Google.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

La patente solicitada por Google en el año 2003, a la cual denominó “patente de generación de información de usuario para su uso en publicidad dirigida”, fue el gran golpe empresarial y tecnológico de la gran empresa de Silicon Valley. Sin embargo, esta patente demuestra que “…la nueva Google hizo caso omiso de esas reivindicaciones de libre determinación individual y no reconoció ningún límite previo a lo que podía encontrar y quedarse” (Zuboff, 2021, p. 117).

Pero la minería de datos debe ser a gran escala para que funcione el producto de predicción de comportamientos, la materia prima debe ser abundante. En tal sentido, la autora detalla que para que el capitalismo de la vigilancia esté en marcha, uno de los principios o imperativos es el extractivismo masivo de datos, muchos, todos, los que más se puedan obtener más allá de su veracidad.

De este modo el proceso de vigilancia se configura de modo unilateral, secreto, con alto valor potencial y real, como también con un gran poder de perjudicar y vulnerar la intimidad de los usuarios.

10. Políticas públicas de salud y seguridad que utilizan IA

10.1 Caso de uso: aplicación para la predicción de embarazos adolescentes en Salta

A continuación, nos referiremos a una tecnología desarrollada con IA. En el año 2018, Juan Manuel Urtubey, gobernador de la provincia de Salta de ese entonces, anunciaba el lanzamiento de un programa de prevención del embarazo adolescente en medios masivos de comunicación de la Ciudad Autónoma de Buenos Aires.

El proyecto sería llevado adelante por el Poder Ejecutivo provincial salteño, a través de su Ministerio de la Primera Infancia y con el desarrollo tecnológico de la empresa de *software* Microsoft. En la presentación mediática de la aplicación, cuenta el funcionario del ejecutivo provincial que con esta herramienta se podría prever con

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

5 años de anticipación, qué mujer, identificada con nombre, apellido y domicilio, quedaría embarazada en los próximos años.

Sin embargo, este sistema de algoritmos despertó algunas alarmas. De acuerdo a la información que pudimos obtener no estaría en uso en la actualidad.

Nos resulta importante señalar algunos puntos sobre la herramienta, y para ello, seguiremos lo planteado por el Laboratorio de Inteligencia Artificial Aplicada de la Universidad de Buenos Aires (IALAB).

En un informe elaborado por el investigador Fernández Slezak, identifica errores técnicos y conceptuales tales como: resultados artificialmente sobredimensionados, ya que los datos evaluados, que son nuevos, incluyen réplicas casi idénticas de muchos datos de entrenamiento. El investigador señala al respecto que:

> ...los datos sobre los que se evalúa el sistema deben ser distintos a los datos que se usan para entrenarlo. Si este principio se viola, es decir, si hay contaminación de datos de entrenamiento en los datos sobre los cuales se valida, los resultados serán inválidos (https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/)

Los datos que se relevaron a través de las encuestas son datos sensibles, a saber: etnia, escolarización, edad, discapacidad, país de origen, embarazos previos, etc. Por tal característica, sostiene el investigador, cabe poner en duda la veracidad de los datos recolectados y usados. Por ejemplo, es probable que un adolescente que ha cursado un embarazo no de esa información.

En tal sentido y a modo de síntesis, compartimos las conclusiones que esboza el investigador, a las que adherimos en razón de lo que venimos manifestando. Diseñar herramientas tecnológicas no puede ser un acto impensado ni menos aún no estudiado, es relevante contar con un análisis del riesgo que pueda ocasionar el programa de *software* o las TIC.s en general.

Al respecto Fernández Slezak (2020) concluye:

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> Tanto los problemas metodológicos como los datos poco confiables plantean el riesgo de llevar a tomar medidas incorrectas a los responsables de políticas públicas. Este caso es un ejemplo de los peligros de utilizar los resultados de una computadora como una verdad revelada. Las técnicas de inteligencia artificial son poderosas y demandan responsabilidad por parte de quienes las emplean. En campos interdisciplinarios como éste, no debe perderse de vista que son sólo una herramienta más, que debe complementarse con otras, y de ningún modo reemplazan el conocimiento o la inteligencia de un experto, especialmente en campos que tienen injerencia directa en temas de salud pública y de sectores vulnerables (párr. 17, https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/)

En este caso en particular la lesión a la autodeterminación informativa proviene del uso de datos sensibles sin el consentimiento informado de los/as titulares de los mismos, para el desarrollo de un *software* de predicción con serios problemas metodológicos y técnicos, que derivan en un programa de IA sembrado de sesgos algorítmicos discriminatorios y de resultados sobredimensionados e inválidos por la contaminación con datos de entrenamiento.

10.2 Caso de uso: Sistema de Reconocimiento Facial de Prófugos (SRFP)

En el próximo caso, analizaremos la implementación del Sistema de Reconocimiento Facial de Prófugos (SRFP), que además contempla un sistema de predicción de situaciones anómalas en el espacio público, desarrollado con un *software* de IA y puesto en funcionamiento en la Ciudad Autónoma de Buenos Aires desde el año 2019.

La ciudad de Buenos Aires fue la primera en todo el país en utilizar un sistema inteligente de estas características, y fundó su decisión en la necesidad de detectar y detener prófugos de la justicia.

Sin embargo, y a pesar de que existen algunos ejemplos a nivel global (Londres, China), se generaron controversias y denuncias cruzadas cuando el sistema tuvo varios falsos positivos. Éstos se tratan de un error en el reconocimiento facial,

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

que indica a los operadores del sistema que se detectó a una de las personas buscadas, cuando en realidad se trata de otra persona.

El sistema fue criticado y denunciado por diversas asociaciones y organizaciones, entre ellas, la Fundación Vía Libre, *Access Now*, Amnistía Internacional, Asociación por los Derechos Civiles, el CELS, DATAS y el Observatorio de Derecho Informático Argentino, los cuales fundan su objeción al programa centralmente en tres puntos: 1) los errores que configuran los falsos positivos; 2) las prohibiciones existentes en otras legislaciones que ya han tenido experiencias similares -San Francisco, Boston, Portland y algunos países de Europa-, y; 3) en la relatoría especial del enviado de la Organización de Naciones Unidas (ONU).

Cabe destacar que la relatoría especial de ONU que visitó el país, consideró que el sistema no podía implementarse sin realizar evaluaciones de impacto en los derechos humanos de los ciudadanos, tal cual lo expresó Joseph Cannataci (2019), el encargado de la relatoría

> …no veo la proporcionalidad de instalar una tecnología con graves implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualmente incluye a menores y delitos no graves y que no se actualice y compruebe cuidadosamente su exactitud (punto 20, https://argentina.un.org/index.php/es/168010-declaracion-del-relator-especial-sobre-el-derecho-la-privacidad-tras-visitar-argentina).

Respecto a los falsos positivos, existen algunos casos graves, como el de Guillermo Ibarrola, que fue detenido tras la detección que realizó el sistema, confundiéndolo con un prófugo, y trasladado a Bahía Blanca, donde estuvo preso por una semana, hasta que se corroboró que no era el criminal buscado.

Este es el tipo de problemas que trae aparejado el uso de IA sin el necesario entrenamiento y auditoría, a los fines de que no vulnere los derechos de los ciudadanos y ciudadanas.

Ante estas situaciones, la Asociación de Derechos Civiles pidió que se declare la inconstitucionalidad del sistema, pero no tuvo éxito, pues el Tribunal Superior de

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Justicia de la Ciudad rechazó el planteo. Más adelante, el Observatorio de Derecho Informático Argentino (ODIA) presentó un amparo colectivo contra el SRFP.

Por otro lado, la función predictiva de la IA sobre situaciones anómalas presenta marcados sesgos en relación a la detección de individuos sospechosos por conducta anómala que, curiosamente, son todos de tez oscura. Beatriz Busaniche, presidenta de la Fundación Vía Libre, expresó al respecto:

> Se implementa un sistema automatizado, basado en el entrenamiento de algoritmos para identificar y levantar alertas sobre situaciones anómalas en la esfera pública. El algoritmo decide qué conductas son anómalas. Eso es una forma muy invasiva de intervención en el espacio público (https://www.lacapital.com.ar/la-ciudad/reconocimiento-facial-via-publica-sesgos-y-prohibiciones-otras-ciudades-del-mundo-n2622511.html).

Nuevamente volvemos al problema de los sesgos algorítmicos por traslación ideológica de los programadores y de las bases de datos que ponen en riesgo o directamente lesionan los derechos fundamentales de ciudadanos y ciudadanas argentinos.

En este particular caso la autodeterminación se ve limitada por el uso irrestricto, inconsulto y arbitrario que realiza este sistema sobre cualquier persona que transite por las calles de la Ciudad Autónoma de Buenos Aires.

Es importante aclarar que este sistema, si bien utiliza cámaras de video para captar información, no funciona como un sistema de vigilancia normal, donde se obtienen simples imágenes, que posteriormente un ser humano o un programa puede interpretar, aquí estamos hablando de una identificación y rastreo a tiempo real de cada persona que detecta la IA, utilizando sus datos biométricos, que son datos personales sensibles, en los términos del art. 2° de la LPDP, sin consentimiento de los titulares, y para un uso expresamente prohibido, que es la identificación de los titulares, conforme lo establece los arts. 7° y 8° de la LPDP.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

La LPDP permite el uso de datos sensibles, pero solo si los titulares dan su expreso consentimiento y exclusivamente para satisfacer un "…interés general autorizado por la ley o si su tratamiento es con fines científicos o estadísticos, con la debida precaución de que los titulares no puedan ser identificado" (art. 7° LPDP).

El sistema vulnera la privacidad de manera flagrante, ya que invade las acciones privadas de las personas que no tienen problemas con la ley ni perjudican a tercero, y como marca el art. 19 de la Constitución Nacional, estas acciones "…están sólo reservadas a Dios, y exentas de la autoridad de los magistrados". Sería absurdo tornar a este derecho nulo en el espacio público por el hecho de que el 1,6% de la población está prófuga de la justicia. No se ajusta a ningún tipo de examen de proporcionalidad.

Nos preguntamos hasta dónde puede el Estado, a través de su poder de policía, restringir el derecho a la privacidad, ¿amerita la búsqueda del 1.6% de la población, es decir, 46.000 prófugos aproximadamente, que se restrinja el derecho a la intimidad y la autodeterminación informativa al 98,4% restante, más de 3 millones de habitantes? La respuesta categórica es no.

El lunes 11 de abril de 2022, el Juzgado de Primera Instancia en lo Contencioso, Administrativo y Tributario N°2 de la C.A.B.A. suspendió el uso del SRFP, fundado en la puesta en marcha del sistema con una ausencia de garantías de supervisión por parte de los organismos de control, la falta de estudio sobre el impacto sobre los datos personales de los ciudadanos y la idoneidad del sistema para el cumplimiento de los objetivos políticos perseguidos.

Además, se remarca que se habría privado a los habitantes y a los/as legisladores/as de intervenir en el asunto, lo que atenta contra el espíritu del orden jurídico porteño. Por otro lado, advirtió un uso de datos biométricos irregular sobre la figura del Presidente y la Vicepresidenta de la Nación, al parecer con el objetivo de

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

realizar un rastreo de sus movimientos (Observatorio de Derecho Informático Argentino O.D.I.A. sobre otros procesos incidentales -Amparo- Otros, 2022).

En conclusión, por el momento el SRFP se encuentra suspendido, pero eventualmente es probable que se vuelva a poner en marcha, e incluso podría extenderse a otros puntos del país. Surge como necesaria la regulación de los sistemas de IA, en especial cuando se implementan desde el Estado y se expone a millones de ciudadanos y ciudadanas a los eventuales daños y perjuicios que puedan emerger de su uso.

11. Seguridad informática

11.1 Casos de uso: filtración masiva de datos de "RENAPER" y de "MercadoLibre"

Seguidamente, analizaremos la mayor filtración de datos de la historia argentina, teniendo en cuenta la cuantía de personas que se vieron afectadas, llegando la cifra hasta los 45 millones de víctimas. Se trata de la filtración del Registro Nacional de las Personas, en adelante RENAPER.

El 11 de octubre del 2021 se da a conocer que el RENAPER había sufrido una vulneración en su base de datos, días después, varios usuarios denuncian que sus datos estaban siendo vendidos en páginas de la *dark web*.

El 24 de octubre del 2021 tomó estado público a través de diversas redes sociales. Un usuario de Twitter, "@aniballeaks", mostró imágenes de los documentos de identidad de políticos, artistas, empresarios y personas de alto perfil.

El Gobierno nacional debió interrumpir el acceso a la red del RENAPER, que está compuesta por más de 50.000 usuarios a lo largo de todo el país, interconectando sistemas municipales, provinciales y nacionales, durante varios días a los fines de auditar su sistema de ciberseguridad e intentar identificar al culpable. Hasta el

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

momento, sólo se pudo descubrir que el usuario “tango11@ jabber” fue el hacker que realizó la infiltración y robo de datos.

Semanas después, el grupo Everest puso a la venta la base de datos del RENAPER por 200.000 dólares. Este grupo se dedica al secuestro de datos personales a través de la encriptación de todo el contenido de una red o equipo informático, tornándola inutilizable para la víctima, y pidiendo un rescate a cambio de la clave de desencriptamiento, modalidad conocida como *ransomware*.

Según el letrado Víctor Castillejo, especialista en derecho informático y entrevistado por iProUP el 25 de noviembre de 2021, “tango11@ jabber” tenía datos actualizados, no sólo del domicilio o número del DNI del letrado, sino que hasta contaba con una foto reciente. "Lo grave es que así como tiene mis datos, tiene también los de cualquier ciudadano argentino. La base de datos se está vendiendo y el RENAPER no hace nada", alertó el abogado.

El presente caso es quizás uno de los más graves, ya que no lesiona únicamente el derecho de autodeterminación informativa de 45 millones de argentinos y argentinas, sino que además los expone a múltiples perjuicios, desde secuestros extorsivos hasta robos de identidad.

Por ahora, RENAPER no ha brindado declaraciones acerca del detalle del ataque informático ni de la extensión de la vulneración, lo que nos hace sospechar que fue tan grave como se cree.

Es necesario remarcar que la filtración y robo de datos es un problema cada día más común en el ciberespacio. Existen sitios en la *dark web* donde es posible contratar a una persona, un hacker, para realizar este tipo de operaciones, a un precio bastante accesible. A su vez, hay distintos eslabones que configuran la cadena criminal del robo de datos: i) los creadores del *software* utilizado para infiltrarse; ii) los que analizan e identifican a las redes más débiles; iii) quienes efectivamente operan

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

el *malware* a fin de realizar el robo de datos y iv) quien contrata y se beneficia con los datos.

Además, esta modalidad delictiva no responde a barreras territoriales, como quedó a la vista con la filtración masiva que sufrió el grupo Cencosud a principios del 2021 por parte del grupo de hackers Egregor, radicados en Ucrania (iProUP, 2021).

En definitiva, asistimos al nacimiento y auge de un nuevo tipo de delitos, ejecutados a través de programas informáticos que utilizan IA, donde el objetivo es el robo o secuestro de bases de datos personales. De confirmarse con la investigación penal en curso, la filtración del RENAPER incluiría los DNI de 45 millones de habitantes, lo que implica que los números de identificación, nombre y apellidos, domicilio, fecha y lugar de nacimiento, firma ológrafa, huella digital, número de trámite y fotografías del rostro están ahora circulando en los rincones oscuros de la web, a la venta al mejor postor, lo que puede derivar en una extraordinaria ola de delitos informáticos contra la población.

Asimismo, remarcamos que el Estado es el responsable de la base de datos y falló en protegerlos. De la misma manera, hay empresas privadas que manejan inconmensurables cantidades de datos personales sensibles y que no están debidamente comprendidos como sujetos responsables en la Ley de Protección de Datos Personales. Tal es el caso, entre otros, de MercadoLibre.

La empresa argentina sufrió el lunes 7 de marzo de 2022 un ataque informático del grupo “Lapsus$”, donde se vulneró el código fuente de la plataforma y se robaron los datos de aproximadamente 300.000 usuarios. Si bien MercadoLibre comunicó que ningún tipo de información sensible fue sustraída, vemos nuevamente cómo el uso de algoritmos con IA para la recolección, proceso y almacenamiento de datos personales de usuarios a los fines de generar perfiles comerciales atrae la atención de grupos de hackers y termina siendo vulnerada y luego vendida en el mercado ilegal.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Es necesario indagar en la interconexión entre el uso de IA y el aumento del riesgo para las bases de datos, ya que los *malware* que utilizan algoritmos automatizados con IA son capaces de infiltrarse, recabar la información necesaria marcada por el programador (*spyware)* y ejecutar las órdenes recibidas de manera autónoma. También son capaces de simular que son una aplicación normal, pero en segundo plano realizar otras operaciones como el robo de datos (troyano). Terminada su misión, pueden simplemente transferir la información a otro servidor y auto borrarse o encriptar todo el sistema para realizar un secuestro extorsivo (*ransomware*), entre otras cosas.

Es creciente la amenaza a los sistemas de seguridad informáticos y muy difícil el rastreo de ciertas técnicas de hackeo, como el envenenamiento de datos, que se enfoca en manipular la información de entrenamiento de algoritmos de IA para permitirle al hacker programar una "puerta trasera" que sortee las defensas del sistema, autores como Culpan (2022) refieren a estas debilidades de seguridad informática.

Por otro lado, y para concluir, en términos económicos se espera que para el 2028 se triplique el mercado global de ciberseguridad de IA, pasando a valer U$D 35 mil millones.

12. Términos y condiciones de uso en los *softwares*

12.1 Caso de uso: la justicia ordena a *WhatsApp* suspender los nuevos términos y condiciones. *Facebook*. *Meta Platforms Inc. Cambridge Analytica*

Como puntapié inicial del siguiente análisis, cabe recordar lo que mencionamos previamente acerca de la ficción del consentimiento informado de los titulares obtenido a través de la aceptación de términos y condiciones de las grandes empresas proveedoras de servicios en internet. Recalcamos que el consentimiento prestado

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

tiene poco de “informado”, pues es sabido que nadie lee los extensos e intrincados contratos.

El caso que analizaremos involucra a una de las empresas más grandes y valiosas del mundo: Meta Platforms, que actualmente es dueña de WhatsApp, Instagram, Oculus, Facebook y un gigantesco conglomerado de otras empresas relacionadas.

Si bien la *big tech* Meta abarca una verdadera constelación de aplicaciones, cada una debería mantenerse independiente de la otra en cuanto al tratamiento de datos personales de los usuarios. Si comparamos las políticas de privacidad de las distintas plataformas que son propiedad de la mega empresa, parece evidente que es Facebook quien recopila y procesa los datos personales de todas las personas usuarias. De hecho, “…la Política de Datos de Instagram detalla que, si cambian la propiedad o el control de la totalidad o de parte de sus Productos o de sus activos, pueden transferir la información al nuevo propietario” (Corvalán, Díaz Dávila y Simari, p. 525).

El 14 de mayo de 2021 la Secretaría de Comercio Interior dictó la Resolución N° 492, ordenándole a WhatsApp LLC y a Meta Platforms Inc., así como a toda otra empresa controlada por ellas, que suspendan la implementación de las “Condiciones de Servicio y la Política de Privacidad de *WhatsApp Messenger*” cuya entrada en vigencia se previó para el 15 de mayo de 2021, en la cual además, les prohíbe intercambiar datos, metadatos y cualquier otro tipo de información de usuarios de WhatsApp con las otras plataformas de Meta.

Posteriormente, a principios del corriente año, la abogada Johanna C. Faliero presentó una denuncia contra WhatsApp por las cláusulas abusivas que tiene en sus políticas de privacidad, logrando que la Dirección de Defensa al Consumidor y Arbitraje de Consumo sancione a la empresa con una multa de cinco millones de pesos.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Tras este revés, la Cámara de Apelaciones en lo Civil y Comercial Federal rechazó el recurso de la empresa contra la Resolución N° 492, prorrogando la suspensión hasta que se finalice la investigación en curso.

Sin ir más lejos, la Agencia Española de Protección de Datos ha multado *a* Facebook y a WhatsApp en el año 2018. A WhatsApp por comunicar datos a su empresa matriz sin autorización de sus usuarios/as y a Facebook por el tratamiento dado a dichos datos para sus propios fines

Lo que importa del presente caso, a los fines de nuestra investigación, es la conexión entre el uso de IA y la lesión a la autodeterminación informativa, y con Facebook, tenemos uno de los casos más graves de toda la historia de internet a nivel mundial: *Cambridge Analytica.*

Es de resonancia y actualidad el caso de la consultora británica que, utilizando los datos personales de más de 50 millones de usuarios, la mayoría estadounidenses, realizó ingeniería conductual y manipulación social y logró contribuir significativamente a la victoria electoral de Donald Trump en 2016.

De modo sintético, comentamos que la IA generaba perfiles psicológicos basados en los datos recolectados en Facebook, a saber: *likes*, historias compartidas, listas de seguidos y seguidores, tiempo de permanencia en pantalla, a los fines de direccionar la propaganda política de manera automatizada y en base al posicionamiento político del usuario generado por el sistema inteligente.

Cambridge Analytica implementó las llamadas operaciones psicológicas (psyops), cuyos objetivos eran lograr modificar la opinión de la sociedad a través de una imposición informativa subrepticia, utilizando técnicas de manipulación social y conductual.

A través de los perfiles creados por la IA de la consultora sabían de qué manera influir imperceptiblemente sobre los usuarios, ya que contaban con la información

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

necesaria para adaptar cada mensaje, la forma, el tema, el contenido, la emotividad y la reiteración del mismo hasta lograr su objetivo.

En una conferencia sobre *big data* y psicografía realizada en 2016, el *CEO*, máximo ejecutivo de la consultora, Alexander Nix, admitió:

> Había equipos de creativos, diseñadores, productores de vídeo, fotógrafos. Ese contenido creado se enviaba a un equipo de targeting, que lo acabaría "inyectando en internet". Se crearían sitios web, blogs, lo que creyéramos que ese perfil objetivo necesitara para ser receptivo, lo crearíamos para que lo encontrase. Y entonces lo verían, harían clic, y seguirían adentrándose en ese agujero hasta que acabaran pensando algo distinto a lo que pensaban (Nix, 2016, min. 8:17).

Pero más allá del caso principal por el cual se conoce a Cambridge Analytica, es menester traer a colación que la empresa también trabajó en la Argentina.

Diversos medios masivos de comunicación, en septiembre de 2019, sacaron a la luz ciertos hechos sobre la actuación de la consultora en el país.

El equipo de investigación de la revista Noticias entrevistó al último CEO de Cambridge Analytica*,* Julian Wheatland, quién confirmó que se realizaron trabajos en territorio argentino, entre ellos, la participación en una elección local. A su vez, Alexander Nix, ex *CEO* y fundador de la empresa, admitió bajo juramento en 2018 ante la Comisión de Asuntos Digitales del parlamento británico haber trabajado en una campaña “antikirchnerista”, pero no reveló la identidad de sus contratantes.

Por otro lado, el periodista Hugo Alconada Mon, en una nota en el diario La Nación, desvela que el partido político Propuesta Republicana (PRO) contrató los servicios de Cambridge Analytica en la antesala de la campaña presidencial, aunque, sin embargo, el acuerdo no se llegó a concretar porque los equipos propios del partido político lograron obtener lo mismo que la empresa les ofrecía.

Más allá de todo esto, nos encontramos nuevamente ante un uso de IA para recabar datos personales sin el consentimiento informado de los titulares. Si bien no sabremos si Cambridge Analytica vulneró los derechos de algún argentino o argentina,

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

debemos prestar atención y poner el foco en los términos y condiciones que imponen las empresas como Facebook (ahora Meta), que, como mostraremos a continuación, son groseramente inconstitucionales.

Si uno accede a las condiciones de uso y a la política de datos de Meta, que abarca a todas sus empresas controladas podemos observar que, como contraprestación a nuestro uso de las aplicaciones, otorgamos a la empresa una licencia "...internacional, sublicenciable, transferible, libre de regalías y no exclusiva para alojar, usar, distribuir, modificar, ejecutar, copiar, mostrar o exhibir públicamente y traducir tu contenido, así como para crear trabajos derivados de él". (https://developers.facebook.com/terms/dfc_platform_terms/?locale=es_LA).

De la misma manera, la *big tech* obtiene un permiso para mostrar nuestro nombre de usuario, foto de perfil, información sobre las acciones que realizamos, nuestras relaciones, las cuentas, anuncios y ofertas que seguimos o con los que interactuamos, sin obligación de proporcionarnos compensación alguna. Sería interesante realizar una encuesta y preguntar a los usuarios de aplicaciones de Meta si conocen lo que están haciendo con sus datos personales, a fin de verificar si se cumple con el consentimiento informado que exige la LPDP.

Continuando el análisis, nos resultan abusivas numerosas cláusulas de la compañía, rozando o cayendo directamente en la inconstitucionalidad. En la práctica, lo que hacemos al utilizar los productos de este tipo de empresas, es concederles la titularidad de nuestros datos personales, enmascarado bajo el rótulo de "licencia internacional", para que hagan lo que crean conveniente, sin tener que informarnos del uso y destino que se le da a los datos, sin volvernos partícipes de cualquier ganancia que se genere por ellos, sin ningún tipo de garantía, excepto las que puedan obtenerse en una disputa legal ante un tribunal, de que responderán por los daños que puedan ocasionar.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

No es menor el hecho de que la empresa Meta tenga bajo su órbita a Facebook, Instagram, Whatsapp y Oculus. Tan solo estas cuatro empresas poseen acceso a los datos de más de 2500 millones de usuarios de todo el mundo. Si no se pone la lupa sobre las acciones y omisiones de este tipo de *big tech* corremos el riesgo de que el ordenamiento argentino que tutela la privacidad, libertad y autodeterminación informativa se torne ilusorio.

Como podemos observar, los privados también tienen un potencial abrumador para generar violaciones masivas de derechos y, por lo tanto, la adopción por parte del Estado de políticas públicas a largo plazo sobre la materia se vuelve indispensable.

La fusión entre IA, intereses comerciales, elecciones y manipulación social es un combo explosivo que debe ser cuidadosamente abordado por el Estado.

13. Derecho al olvido: breve conceptualización

Al día de hoy, nuestra identidad es dual, por un lado, tenemos nuestra identidad física, que se conforma a través del cuerpo, la imagen, las ideas que tenemos, las acciones que emprendemos, la autopercepción, entre otros. Por otro lado, desde que comenzamos a interactuar con internet, cada dato y metadato que generamos coadyuva a la construcción de una identidad digital, que muchas veces, dice más de nosotros mismos que nuestra propia identidad física.

La autodeterminación informativa surge ante la necesidad de tener control sobre esos datos y metadatos que generamos constantemente. Pero ¿qué ocurre cuando esos datos dejan de ser privados y toman conocimiento público, despertando el interés de la sociedad? ¿Qué sucede si el titular de los datos personales decide restringir el acceso público a los mismos? Aquí es donde entra el derecho al olvido y el caso que veremos a continuación.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Es importante destacar la tensión que existe aquí: por un lado, tenemos la autodeterminación informativa de los titulares sobre sus datos personales, enmarcado por el derecho a la intimidad y al honor, y en otro extremo, tenemos el derecho a la libertad de información y expresión de la sociedad sobre temas que despierten el interés público, lo que engloba el derecho a la historia, la verdad y el conocimiento de la realidad humana (Faliero, 2020).

Ahora bien, ambos derechos son fundamentales, tienen categoría de derecho humano, están reconocidos constitucionalmente, así como convencionalmente, tienen una arista individual y una colectiva y requieren una adecuada ponderación para garantizar su ejercicio.

Por otra parte, es preciso definir el derecho al olvido. En la liza donde se cruzan el mundo físico y el digital, donde los datos personales se convierten en información, surge la necesidad de los titulares de tener derecho a la privacidad, armonizado con el derecho a la libertad de expresión de los demás, ya que, recordemos, los derechos no son absolutos. En otras palabras, el derecho a ser olvidado emerge como un punto medio entre ambos derechos, donde, transcurrido cierto tiempo o verificada la ilegalidad o sensibilidad del contenido de los datos, la libertad de información se restringe para salvaguardar los derechos fundamentales del perjudicado.

Es importante destacar que "...la búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de internet, se considera comprendido dentro de la garantía constitucional que ampara la libre expresión" (art. 1°, ley 26.032), así como que:

> El derecho de expresarse a través de Internet fomenta la libertad de expresión tanto desde su dimensión individual como colectiva. Así, a través de Internet se puede concretizar el derecho personal que tiene todo individuo a hacer público, a transmitir, a difundir y a exteriorizar —o no hacerlo— sus ideas, opiniones, creencias, críticas, etc. Desde el aspecto colectivo, Internet constituye un instrumento para garantizar la libertad de información y la formación de la opinión pública (Declaración Conjunta sobre Libertad de Expresión e Internet

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> de la Relatoría para la Libertad de Expresión de la OEA, 1º de junio de 2011, párr. 4).

En la Argentina existen varios fallos que sentaron jurisprudencia acerca de este derecho y cómo se debe accionar al respecto, ya que no es un derecho regulado en nuestro ordenamiento de manera específica. Es un aporte muy valioso para analizar el impacto de un sistema de IA como el de Google sobre el derecho a la autodeterminación informativa de los titulares de los datos personales en los que se funda la información proveída por los buscadores.

En otras regulaciones, como lo afirma Failero (2020), por lo general y desde la protección de datos personales, el derecho al olvido se maneja por vía de la supresión de datos personales, como instituto análogo y derecho del titular del dato.

13.1 Caso "Rodríguez"

El primer fallo que analizaremos brevemente será el de **"**Rodríguez María Belén c/ Google Inc s/ Daños y Perjuicios" de la Corte Suprema de Justicia de la Nación (CSJN), del año 2014.

En este caso, la actora promovió una demanda por daños y perjuicios contra la empresa por el uso comercial no autorizado de su imagen y su vinculación con páginas web de contenido pornográfico.

En el decisorio, los supremos interpretaron que los motores de búsqueda tienen responsabilidad subjetiva respecto a las eventuales responsabilidades emergentes de los daños y perjuicios ocasionados, toda vez que son meros intermediarios entre usuarios y proveedores. Por lo tanto, para que surja la responsabilidad en cabeza de los buscadores, deben haber tenido conocimiento efectivo de un contenido ilícito en una página web sin haberlo bloqueado de sus resultados de búsqueda, configurando así un causal de culpa, en los términos del art. 1109 del Código Civil y Comercial de la Nación.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

Por otro lado, la mayoría de magistrados no atribuyó responsabilidad por la ausencia de consentimiento informado de los titulares de los datos en la publicación de imágenes de ellos, puesto que entendieron que los buscadores no son responsables por los contenidos de las páginas web. Sin embargo, los Dres. Lorenzetti y Maqueda, en disidencia, entendieron que sí existía responsabilidad, toda vez que los buscadores utilizan, almacenan y reproducen imágenes publicadas por terceros, con la posibilidad de ser descargadas o impresas desde el mismo buscador y, por lo tanto, son sujetos responsables por el tratamiento de datos personales (art. 31, Ley 11.723).

Finalmente, desestiman la demanda por completo, sin otorgar el derecho al olvido a la actora.

13.2 Caso "Gimbutas"

En el caso **"**Gimbutas, Carolina Valeria c/ Google Inc. s/ Daños y perjuicios"**,** de la CSJN, del año 2017, de manera similar a lo ocurrido en el fallo anterior, la modelo Carolina Gimbutas demandó a Google por la vinculación que realizaban los algoritmos de IA entre su nombre y sitios de contenido pornográfico, así como por el uso indebido de su imagen y otros datos personales.

En este caso, la mayoría nuevamente confirmó lo sentado en el precedente Rodríguez, fundado sobre la irresponsabilidad de los buscadores por su carácter de meros intermediarios, ajenos al contenido publicado en los sitios web, en tanto no tomen conocimiento de la ilicitud o dañosidad de las publicaciones y no actúen en consecuencia.

Respecto a la reproducción de imágenes de la actora en la búsqueda por imágenes del buscador de la empresa demandada, consideraron que no puede entenderse que las mismas hayan sido editadas y puestas en el comercio en el sentido del art. 31 de la ley 11.723, que exige el consentimiento expreso del titular, y el inciso

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

c) del artículo 53 del Código Civil y Comercial de la Nación entra en consideración, teniendo en cuenta que permite la reproducción de la imagen de una persona sin su consentimiento cuando ésta participe de actos públicos o la reproducción esté enmarcada en el ejercicio regular del derecho de informar sobre acontecimientos de interés general.

Nuevamente, desestiman por completo la pretensión de la actora. En esta ocasión, también nos encontramos con las disidencias de los magistrados Lorenzetti y Maqueda, quienes entienden que, al igual que en el fallo Rodríguez, el buscador utilizó imágenes de la actora sin su consentimiento, lo que configura una invasión a la esfera íntima que debe ser reparada (Gimbutas, Carolina Valeria c/ Google Inc. s/ daños y perjuicios, 2017).

13.3. Caso "Pompilio"

El tercer caso que veremos, "Pompilio, Natalia Andrea c/ Google Inc. s/ habeas data (art. 43 Constitución Nacional), de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala II, del año 2021, trata sobre la denuncia de Natalia Pompilio contra Google para que suprima de sus bases de datos los datos personales de su padre, Pedro Pompilio -en adelante P.P.- en relación a los resultados de búsqueda que vinculan su fallecimiento con un encuentro sexual inexistente con Jesica Cirio, en manifiesta violación a los artículos 4°, calidad de los datos y 5° consentimiento informado del titular de la LPDP.

En el decisorio, el Tribunal recordó lo sentado por la Corte respecto a:

> ...el caso de personajes célebres cuya vida tiene carácter público o de personajes populares, su actuación pública o privada puede divulgarse en lo que se relacione con la actividad que les confiere prestigio o notoriedad y siempre que lo justifique el interés general. Pero ese avance sobre la intimidad no autoriza a dañar la imagen pública o el honor de estas personas y menos sostener que no tienen un sector o ámbito de vida privada protegida de toda intromisión. Máxime cuando con su conducta a lo largo de su vida, no han fomentado las indiscreciones ni por propia acción, autorizado, tácita o

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> expresamente la invasión a su privacidad y la violación al derecho a su vida privada en cualquiera de sus manifestaciones" (Fallos: 306:1892, considerando 9, Causa n° 5282/2017 "Ponzetti de Balbín, Indalia c. Editorial Atlántida, S.A. s/ Daños y Perjuicios", del 11/12/84).

Siguiendo esta línea, consideraron que al tener un conocimiento efectivo de la ilicitud de la información que proveía su motor de búsqueda, Google es responsable por los daños ocasionados, en virtud de culpa por negligencia, al omitir su deber de prevenir daños. En este sentido, ordenan a la empresa bloquear las URLs que fueron denunciadas por la actora siempre que hagan referencia a la información vinculada al fallecimiento de Pedro Pompilio. (Pompilio, Natalia Andrea c/ Google Inc. s/ Habeas data (Art. 43 C. N.), 2021)

13.4 Caso "Denegri"

El último de los casos que analizaremos está en tratamiento actualmente por la CSJN, y por ahora subsiste lo decidido por la Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, Sala H, en 2020. Es el fallo "Denegri, Natalia Ruth c/ Google Inc. s/ derechos personalísimos: acciones relacionadas".

En el presente, la actora promovió una demanda contra Google solicitando que se aplicara el derecho al olvido respecto de información personal ocurrida más de veinte años atrás y que actualmente le ocasiona graves perjuicios a su honor e imagen personal. A su vez, remarcó que en la actualidad los hechos periodísticos vinculados a la causa penal que son el objeto de la información impugnada carecen de relevancia e interés público y, por lo tanto, no se afectaría el derecho a la información y expresión de terceros.

En su contestación, Google invocó su propia ajenidad, como motor de búsqueda, respecto de los contenidos cuestionados por la actora y que se encuentran subidos a la web por terceros en cuyo respecto Google no ejercería ningún control acerca de la veracidad, la calidad y los alcances de sus contenidos, describió el

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

mecanismo operativo de los buscadores de internet y del servicio denominado Youtube e invocó la protección constitucional del servicio de búsqueda por internet, argumentando acerca de los motivos jurídicos de tal protección.

Asimismo, agrega que la actora debió demandar a los medios que difundieron las noticias, y sostiene que ella participó voluntariamente en programas mediáticos, sabiendo la exposición a la que se sometía, y que lo sucedido en ellos de ninguna manera invade la esfera de la intimidad ni del honor de la actora.

Google indicó que el reclamo de la actora debía redireccionarse contra los sujetos responsables del contenido subido a internet y no contra los buscadores y consideró que en el caso no se había ocasionado daño alguno a los derechos personalísimos de la actora a raíz de su obrar. Al respecto de la supuesta irrelevancia de la cuestión postulada por la actora, sostuvo que estos eran sucesos de innegable interés público que la ciudadanía tiene derecho a conocer y tener disponible. En relación con ello, argumentó acerca del rango constitucional de la protección del derecho a la información y objetó la aplicabilidad al caso bajo examen del denominado derecho al olvido invocado por la peticionaria.

En el decisorio, el Tribunal considera que la reproducción de la información impugnada por la actora no representa interés periodístico alguno, sino más bien parece hallarse fundada en razones de morbosidad, ya que los videos cuestionados se limitan a exhibir escenas grotescas de nulo valor cultural o histórico. Bajo este argumento, admiten la desindexación solicitada por la actora respecto de los eventuales enlaces que puedan exhibir videos e imágenes obtenidos hace veinte años o más que contengan escenas protagonizadas por la actora cuyo contenido muestre "...peleas, agresiones verbales o físicas, insultos, discusiones en tono elevado, escenas de canto y/o baile de precaria calidad artística" (p. 4).

Por otro lado, nos resulta sumamente interesante el planteo del Juez Kiper, a quien los restantes magistrados adhieren en sus votos, cuando expone que:

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

> Hay que observar que si una persona se considera afectada y le pide al buscador que quite de sus búsquedas tal información supuestamente lesiva, eso no impide que el ofensor siga haciéndolo. Por ende, si alguien pretende difundir sus ideas, aún ofensivas, a través de internet, no será censurado. De lo que se trata es de que las demandadas no amplíen o difundan la opinión de un tercero que puede causar un daño ("Denegri, Natalia Ruth C/ Google Inc S/ Derechos Personalísimos: Acciones Relacionadas", 2020, p. 6).

A su vez, el magistrado plantea que el derecho al olvido, si bien no está expresamente regulado en el orden jurídico, puede ser una valiosa herramienta para hacer valer los derechos al honor y la intimidad, lo que nos devuelve al punto de partida, la autodeterminación informativa, y su vínculo indubitable con ambos derechos.

Sin embargo, Kiper aclara seguidamente que "...el derecho al olvido, interpretado de un modo no restrictivo, puede implicar una terrible pérdida de historia y cultura con efectos colaterales imprevisibles e incontenibles a nivel colectivo…" (p. 11) y, por lo tanto, debe ser aplicado irremediablemente de forma restrictiva, encontrando un punto medio entre los derechos en tensión.

En este particular caso de estudio, el uso de IA de los motores de búsqueda por internet ha ocasionado numerosos conflictos con la autodeterminación de los titulares de los datos, al vincular, en ocasiones sin motivos aparentes, datos entre sí, causando una violación a la esfera privada de las personas y omitiendo el esencial consentimiento informado que requiere el tratamiento de tales datos. Sin embargo, se plantea una situación peculiar, debido al rol de intermediarios de los motores de búsqueda, que son ajenos al contenido de los enlaces que ellos proveen.

Por lo tanto, consideramos necesario el tratamiento legislativo del derecho al olvido, a los fines de determinar con precisión los presupuestos que lo habilitan y la reglamentación del mismo, para así lograr un equilibrio saludable entre la libertad de expresión y la autodeterminación informativa, contemplando el tratamiento automatizado de los datos que realizan los algoritmos de IA de los buscadores.

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

14. Conclusión

Finalmente podemos concluir que si bien en la actualidad la mayoría de las IAs que hay funcionando responden a la caracterización de débiles, más ligadas a procesos de automatización que a verdaderas inteligencias virtuales *pseudo* humanas, su potencialidad implica numerosos riesgos que deben tenerse en cuenta a la hora de legislar la tutela del derecho reseñado que, si bien no cuenta con una conceptualización propia en el ordenamiento argentino, contamos con una batería de leyes que protegen a los titulares de datos personales ante la creciente amenaza del extractivismo masivo por parte de la *big tech*.

Debemos estar muy atentos a la aparición de nuevas IAs en la disruptiva evolución tecnológica, que, de manera aritmética, crecen exponencialmente, con el afán de mantener el esquema de derechos fundamentales protegidos, sin quedar a la zaga en la carrera tecno-industrial propugnada por la globalización capitalista contemporánea.

Cabe destacar el importante aporte al campo del derecho que viene realizando la Unión Europea en cuanto a la regulación y protección de datos personales, así como de la implementación de inteligencias artificiales en el mercado.

Esperemos que la Argentina en particular, y los países en vías de desarrollo en general, no sean nuevamente un escenario de experimentación para los proyectos potencialmente peligrosos que los países centrales no pueden ni quieren probar en sus territorios.

Como investigadores e investigadoras del derecho estará en nuestra mano contribuir al desarrollo armónico del avance científico en conjunto con el crecimiento social justo y sostenible.

Con esta investigación nos proponemos ofrecer un análisis desde una perspectiva legal sobre el desarrollo de aplicaciones móviles y programas de

Ratio Iuris. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151

computación desarrolladas con tecnología de IA, las cuales son utilizados en políticas públicas.

Además, intentaremos brindar una serie de indicadores objetivos a modo de protocolos, como herramientas coordinadas y adecuadas a derecho, para el diseño, planificación e implementación de las políticas públicas. Siempre teniendo como faro el análisis del impacto de estas tecnologías con relación al ejercicio de los derechos fundamentales.

15. Bibliografía y fuentes de información

15.1 Bibliografía

Barocas, S., & Selbst, A. (2016). Big Data's Disparate Impact [Impactos desiguales del Big Dat]. En *California Law Review*, 671-732. http://dx.doi.org/10.15779/Z38BG31

Benítez, R., Escudero, G., Kanaan, S., & Masip Rodó, D. (2013). *Inteligencia artificial avanzada.* UOC.

Bertola, L. (3 de junio de 2022). *El Gobierno porteño juega al Gran Hermano*. https://www.pagina12.com.ar/414310-el-gobierno-porteno-juega-al-gran-hermano?ampOptimize=1

Busaniche, B. (11 de noviembre de 2020). *Reconocimiento facial en vía pública: sesgos y prohibiciones en otras ciudades del mundo.* https://www.lacapital.com.ar/la-ciudad/reconocimiento-facial-via-publica-sesgos-y-prohibiciones-otras-ciudades-del-mundo-n2622511.html

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Corvalán, J. G. (2021). *Tratado de inteligencia artificial y derecho.* La Ley.

Corvalán, J., Díaz Dávila, L., & Simari, G. (2021). Inteligencia Artificial: Bases conceptuales para comprender la revolución de las revoluciones. En J. Corvalán (dir). *Tratado de Inteligencia Artificial y Derecho* (Tomo I, pp. 15-68). Thomson Reuters.

Cotino Hueso, L. (2019). Riesgos e impactos del big data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo 50*.

Culpan, T. (24 de abril de 2022). *The Next Cybersecurity Crisis: Poisoned AI*. [La próxima crisis de ciberseguridad: IA envenenada]. https://www.bloomberg.com/opinion/articles/2022-04-24/ai-poisoning-is-the-next-big-risk-in-cybersecurity

Faliero, J. (2020). Los peligros del derecho al olvido digital: cuando la autodeterminación informativa colisiona con él. La ley, AR/DOC/653/2020.

Fernández, Y. (11 de septiembre de 2017). *Multa de 1,2 millones de euros a Facebook: Protección de Datos carga contra sus perfiles en la sombra*. https://www.xataka.com/servicios/multa-de-1-2-millones-de-euros-a-facebook-proteccion-de-datos-carga-contra-sus-perfiles-en-la-sombra

Gil, E. (2016). *Big Data, privacidad y protección de datos.* Agencia Española de Protección de Datos.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Hao, K. (2019). *Cómo se produce el sesgo algorítmico y por qué es tan dificil detenerlo.* https://www.technologyreview.es/s/10924/como-se-produce-el-sesgo-algoritmico-y-por-que-es-tan-dificil-detenerlo

Kaku, M. (2013). *La física del futuro. Cómo la ciencia determinará el destino de la humanidad y nuestra vida cotidiana en el siglo XXII.* Debolsillo.

Kurzweill, R. (2013). *Cómo crear una mente: El secreto del pensamiento humano.* Lola Books.

Molina Quiroga, E. (2003). *Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material*. http://www.saij.gob.ar/eduardo-molina-quiroga-proteccion-datos-personales-como-derecho-autonomo-principios-rectores-informes-solvencia-crediticia-uso-arbitrario-dano-moral-material-dacc030027-2003/123456789-0abc-defg7200-30ccanirtcod

Musk, E. (2018). Elon Musk Answers Your Questions [Elon Musk responde tus preguntas]. https://www.youtube.com/watch?v=kzlUyrccbos

Nix, A. (2016). The Power of Big Data and Psychographics [El poder de la big data y la psicografía]. Concordia Annual Summit.

Oszlak, O., & O'Donnell, G. (1976). *Estado y políticas estatales en América Latina: hacia una estrategia de investigación.* CEDES. https://www.studocu.com/es-

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

ar/document/universidad-del-salvador/politicas-turisticas/oszlak-y-o-donnell-estado-y-politicas-estatales/11941822

Pastor, J. (2018). *El escándalo de Cambridge Analytica resume todo lo que está terriblemente mal con Facebook*. https://www.xataka.com/privacidad/el-escandalo-de-cambridge-analytica-resume-todo-lo-que-esta-terriblemente-mal-con-facebook

Riande Juárez, N. A. (2022). *El derecho a la autodeterminación informativa.* https://www.tfja.gob.mx/investigaciones/historico/pdf/elderechoalaautodeterminacion.pdf

Rusell, S., & Norvig, P. (2016). *Artificial Intelligence -a modern approach* [Inteligencia Artificial una moderna contemporánea] (3a ed). Prentice Hall.

Sánchez Caparrós, M. (2021). Inteligencia artificial, sesgos y categorías sospechosas. Prevenir y mitigar la discriminación algorítimica. En J. Corvalán. *Tratado de Inteligencia Artificial y Derecho* (pp. 299-321). La Ley.

Sanchez, J. (2020). Así funcionan los sesgos de la inteligencia artificial. *ABS Soluciones*. https://www.abc.es/tecnologia/informatica/soluciones/abci-funcionan-sesgosinteligencia-artificial202009130134_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Vercelli, A. (2021). El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto. *Revista de Derecho 79,* 111-125.

Warwick, K. (2012). *Artificial Intelligence: the basics* [Inteligencia Artificial: las bases]. Routledge, Taylor & Francis Group.

Zuboff, S. (2021). *La era del capitalismo de la vigilancia*. Paidós.

15.2 Fuentes de información

CN de Apelaciones en lo Civil de la Capital Federal, agosto de 2020, “Denegri, Natalia Ruth C/ Google Inc S/ Derechos Personalísimos: Acciones Relacionadas”, expte. 50016/2016.

CNF de Apelaciones en lo Civil y Comercial, Sala II, abril de 2021, Pompilio, Natalia Andrea c/Google Inc. s/ habeas data (art. 43.CN), Causa n° 5282/2017.

Constitución Nacional Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

CSJN, 28 de octubre de 2014, "Rodríguez, María Belén el Google Inc. s/ daños y perjuicios", R. 522. XLIX.

CSJN, 12 de octubre de 2017, “Gimbutas, Carolina Valeria c/ Google Inc. s/ daños y perjuicios”.

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Decreto 1089/2012. reglamentación de la Ley Nº 26.529. https://e-legis-ar.msal.gov.ar/htdocs/legisalud/migration/html/19537.html

Decreto 1172/2003. Acceso a la información pública. http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/90763/texact.htm

Decreto 1225/2010 Servicios de comunicación audiovisual. http://servicios.infoleg.gob.ar/infolegInternet/anexos/170000-174999/171306/norma.htm

Decreto 1558/2001. Protección de los datos personales. https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368/actualizacion

INFOBAE, (15 de marzo de 2018). *WhatsApp y Facebook, sancionados por el uso y tratamiento que hacen de la información de sus usuarios*. https://www.infobae.com/america/tecno/2018/03/15/whatsapp-y-facebook-sancionados-por-el-uso-y-tratamiento-que-hacen-de-la-informacion-de-sus-usuarios/

iProUP. (19 de 2 de 2021). *Hackeo a Disco, Easy y Jumbo: desbaratan la banda que robó datos de clientes a Cencosud*. https://www.iproup.com/economia-digital/20711-desactivan-la-banda-que-robo-todos-los-datos-de-cencosud

iProUP. (25 de 11 de 2021). *Un escándalo que el Gobierno quiere esquivar: qué se sabe del mayor robo de datos de personas en Argentina*.

https://www.iproup.com/innovacion/27351-filtracion-renaper-que-se-sabe-del-robo-de-datos#:~:text=El%2024%20de%20octubre%2C%20el,artistas%20reconocidos%2C%20entre%20muchos%20otros

iProUP. (06 de 01 de 2022). *Argentina le gana la pulseada a WhatsApp y le cobrará una multa millonaria*. https://www.iproup.com/innovacion/28739-whatsapp-multa-en-la-argentina-por-sus-condiciones-de-privacidad

iProUP. (2022). *Facebook sufre otro revés: la Justicia frenó el uso de los datos privados de WhatsApp*. Obtenido de https://www.iproup.com/innovacion/31076-whatsapp-la-justicia-freno-el-uso-de-los-datos-privados

Juzgado de 1ra Instancia en lo Contencioso Administrativo y Tributario n° 2., Sec. 3,11 de Abril de 2022, “Observatorio de Derecho Informático Argentino- O.D.I.A. s/ otros procesos incidentales- Amparo-otros NC 182908/2020-3. https://www.pensamientopenal.com.ar/fallos/90023-caba-suspension-del-sistema-reconocimiento-facial-busqueda-profugos

La Nación. (8 de 3 de 2022). *Mercado Libre confirma la filtración de datos de 300.000 usuarios*. https://www.lanacion.com.ar/tecnologia/mercado-libre-confirma-la-filtracion-de-datos-de-300000-usuarios-nid07032022/

Ley 25.326. Protección de los datos personales. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

Ley 26.206. Ley de Educación Nacional. http://servicios.infoleg.gob.ar/infolegInternet/anexos/120000-124999/123542/texact.htm

Ley 26.522. Servicio de Comunicación audiovisual. http://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/158649/texact.htm

Ley 26.529. Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud. http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160432/norma.htm

Ley 27.078. Argentina Digital http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm

Ley 27.275. Derecho de acceso a la información pública http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-

Ministerio de Desarrollo Productivo, Secretaría de Comercio Interior, Resolución 224/2022 / medida cautelar contra WHATSAPP LLC y META PLATFORMS INC. https://www.petittoabogados.com.ar/blog/2022/03/28/ministerio-de-desarrollo-productivo-secretaria-de-comercio-interior-resolucion-2242022-medida-cautelar-contra-whatsapp-llc-y-meta-platforms-inc/

***Ratio Iuris*. Revista de Derecho. Vol. 10 Núm. 1, enero-junio 2022, pp. 442-504, ISSN: 2347-0151**

OCDE. (2019). Inteligencia artificial en la sociedad. https://www.oecd-ilibrary.org/sites/603ce8a2-s/index.html?itemId=/content/component/603ce8a2-es

ONU. (2020). Resolución 73/348 de la Asamblea General, p. 4. http://undocs.org/es/A/73/348

Organización de Consumidores y Usuarios. (7 de marzo de 2018). *La fuerza de tus decisiones.* https://www.ocu.org/organizacion/prensa/notas-de-prensa/2018/privacidad070318

TSJ de Córdoba, 19 de marzo de 2015, Sentencia n 48, “C.L.A S/ Ejecución de pena privativa de la libertad - Recurso de Inconstitucionalidad.