Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: Su Majestad, el algoritmo: la era de la inteligencia artificial (2015-2020)

Autores (en el caso de tesistas y directores):

Melissa Noelia Bargman

Henoch Aguiar, tutor

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2021

UBA Sociales
FACULTAD DE CIENCIAS SOCIALES

Tesina de Grado

“Su Majestad, el Algoritmo: La era de la Inteligencia Artificial”(2015-2020)

Melissa Noelia Bargman

37.806.185

melibargman93@gmail.com

Tutor: Henoch Aguiar

Dedicado a mis padres, Lía y Claudio,
pilares del apoyo y afecto más incondicional.

Índice

Introducción

Presentación del tema

Los algoritmos atraviesan nuestra vida. Cada vez más comportamientos de todos los días se encuentran vinculados a dispositivos tecnológicos y aplicaciones. Muchas de las decisiones que tomamos, desde qué camino seguir a la mañana hasta qué pedir en el almuerzo o con quién salir un fin de semana están mediadas por el uso de plataformas.

La información que vemos en la pantalla es seleccionada, filtrada y clasificada de acuerdo a los datos que nosotros mismos proporcionamos: lo que consultamos en los buscadores de Internet, los lugares en los que vivimos o visitamos, las publicaciones a las que reaccionamos, las series que nos entretienen. Somos generadores de datos.

Esta masa infinita de información es estudiada y procesada automáticamente a través de algoritmos, una secuencia de pasos o reglas finitas, que se aplican sobre un conjunto de datos de entrada para resolver un problema. Estas instrucciones claramente definidas y programadas constituyen la base sobre la que se desarrolló y expandió el campo de la Inteligencia Artificial (IA) que busca delinear y perfeccionar el aprendizaje automatico de las máquinas (*machine learning*).

Cuanto mayor es el volumen de datos que se recolectan de los comportamientos, más acertada será la creación de los perfiles de usuarios: la materia prima sobre la cual se concentran el marketing y la publicidad. Progresivamente, se desarrollan métodos de análisis y búsqueda de patrones sobre el llamado Big data**.** A diferencia de las técnicas tradicionales de recolección de datos (como por ejemplo las encuestas o llamadas telefónicas para responder cuestionarios de manera voluntaria), Big Data se caracteriza por su espontaneidad y el carácter involuntario con el que las personas generan esa información a medida que usan plataformas.

Cabe preguntarse si las empresas que están detrás del desarrollo y actualización de las plataformas digitales ofrecen a los usuarios instancias claras para informar las políticas de privacidad, seguridad y condiciones de uso de los datos.

Cuando se hace clic en el casillero para aceptar los términos y condiciones de una red social o de uso del Wi-Fi de un espacio público, se da consentimiento personal para que las aplicaciones puedan hacer uso del GPS, la cámara y el micrófono de un dispositivo móvil, ¿se sabe realmente qué y a quién accede a todas estas fuentes?

Si nos descargamos una aplicación o accedemos a un sitio web a través de Facebook ¿queda claro que esa página o aplicación puede acceder a toda nuestra información alojada en la red social y hasta la de nuestros amigos o seguidores?, ¿qué mecanismos de protección se aplican para salvaguardar esos datos y evitar que caigan en las manos equivocadas?

Las plataformas digitales almacenan datos considerados legalmente como sensibles. Esta categoría distintiva exige que su acceso sea reservado y limitado por el impacto que puede significar en la vida de una persona que sean difundidos.

Lo que compramos, el número de nuestras tarjetas de crédito, dónde trabajamos, con quién nos juntamos, nuestros hobbies y gustos, opiniones políticas y hasta con qué personas hablamos más a diario son algunos de los datos que cedemos voluntariamente y quedan en manos de empresas que los almacenan en servidores: infraestructuras digitales que pueden ser vulneradas así como las de las centenares de empresas con las que comparten los datos de los usuarios.

Planteamiento del problema y preguntas de investigación

El ecosistema de plataformas en la economía digital[1] conforma un mercado con una fuerte tendencia a la concentración monopólica. En el caso de Facebook, su co-fundador y presidente, Mark Zuckerberg, no sólo maneja la red social más utilizada a nivel mundial sino que también adquirió Instagram en el año 2012 y Whatsapp en 2014. La gestión y el funcionamiento de las principales plataformas digitales de interacción social contemporánea quedan en manos de un único actor en el cual se concentran los millones de datos que se generan de los usuarios con cada *like*, post o clic que realizan.

Las plataformas resaltan que su uso es gratuito, lo cual está lejos de ser cierto: los usuarios "pagan" con la información que registran cada vez que publican una actualización de estado, escriben una recomendación, dan un "Me gusta", activan la geolocalización, buscan una página en internet. Se conforman cúmulos de datos que son procesados y vendidos para fines que muchas veces rebalsan los publicitarios.

Se trata de un mercado en el que la materia prima es la información de los usuarios. ¿Cuáles son las implicancias de una posición dominante dentro de un mercado con estas características? Los algoritmos en sí mismos son sólo sucesiones de pasos a seguir, pero ¿para qué fines fueron configurados cuando definen los contenidos que se le muestran al usuario en base a sus preferencias o actividad en redes sociales? Si hay pocos actores en el desarrollo de estas tecnologías, también serán pocos los que definan cómo se filtra la información, qué puede mostrarse (y sobre todo, ocultarse) y en qué momento.

No se trata solamente de pensar en los datos que los usuarios generan por su actividad en el mundo digital. En las principales ciudades del mundo (en la Ciudad de Buenos Aires, desde abril de 2019) se implementan tecnologías de reconocimiento facial. Los ciudadanos, sin ser conscientes, son monitoreados por miles de cámaras. Dejan registro de la mayoría de los lugares por los que circulan o de las personas con las que interactúan. La inteligencia

[1] La economía digital está conformada por "los negocios que dependen cada vez más de la tecnología de información, datos e Internet para sus modelos de negocios" (Srnicek, 2018, p 12).

artificial entrecruza esta información con bases de datos biométricos para detectar sospechosos buscados por la justicia. Pero todos los ciudadanos son observados. Nuestros rostros se convierten en las nuevas huellas digitales. Complejos algortimos comparan nuestras características físicas con imágenes almacenadas en algún servidor. ¿Quiénes son los dueños de esos servidores que resguardan y hacen tratamiento de las características de millones de personas?, ¿qué garantiza la protección de esa información?, ¿qué ocurre cuando se comparten nuestras imágenes?, ¿en qué lugar queda el derecho de propiedad de la propia imagen?

Se hace necesaria la creación de nuevas regulaciones o actualización de los marcos vigentes para adaptarse a las nuevas formas de comunicación social. El objetivo es garantizar la privacidad de los usuarios sin minar la libertad de expresión en un entorno extremadamente dinámico y cambiante. Resulta indispensable crear instancias y mecanismos regulatorios que controlen las prácticas y maniobras de los actores que manejan estos mercados.

Las redes sociales no son ni buenas o malas. Se internalizaron en la vida de las personas para facilitar los procesos de la vida cotidiana. La propuesta es poder configurar y conformar un entorno legal que garantice la protección de la intimidad de los usuarios sin vulnerar sus derechos. El mundo se encuentra inserto en una nueva etapa de desarrollo económico, la Sociedad del Conocimiento o Era Digital en la que “el principal generador de valor económico es el saber, el valor agregado intelectual a las cosas y a las acciones” (Aguiar, 2007, p. 21). Esto implica utilizar a la tecnología como aliada facilitadora de procesos y soluciones, y no como una enemiga cuyo fin último es el robo y venta de datos.

Las plataformas digitales se implementaron en todo tipo de prácticas, más allá del entretenimiento o comercio on line: desde el sector médico (reservorios de datos en los que se almacenan historias médicas, antecedentes, resultados de estudios y análisis, diagnósticos) hasta el ámbito educativo (bases de datos con información de rendimiento académico, conducta, datos de menores de edad). Se generan registros de datos sensibles cuya confidencialidad debería ser garantizada por las empresas que desarrollan estos sistemas de bases de datos.

Al tratarse de un mercado que tiende a formar monopolios ¿hasta qué punto se aseguran niveles de innovación y actualización suficientes que logren mejores/mayores estándares de seguridad y de experiencia del usuario si no hay competencia?

Objetivo general de la tesina

El presente trabajo se propone delinear los principales conceptos que conforman el campo de la Inteligencia Artificial, su aplicación en la vida cotidiana y los nuevos desafíos que encarna en la sociedad.

Objetivos específicos

1. Definir los elementos que conforman la Inteligencia Artificial, sus mecanismos de funcionamiento y su evolución histórica.
2. Describir las aplicaciones prácticas en la vida cotidiana desde el sector privado y el Estado en los procesos burocráticos, y en su relación con la ciudadanía.
3. Comparar en materia de normativa el Reglamento General de Protección de datos personales de la Unión Europea (RGPD), vigente desde 2018, con la Ley de Protección de datos personales 25.326 de Argentina sancionada en el año 2000.
4. Estudiar los fenómenos de vigilancia de la ciudadanía por parte del Estado al implementar las nuevas tecnologías.
5. Comprender las nuevas lógicas de funcionamiento de la economía digital.

Metodología

La tesis realiza una investigación de tipo comparativa y sincrónica para explorar los marcos regulatorios vigentes y en debate en materia de protección de datos personales e Inteligencia Artificial. Se hace hincapié en los marcos legales de la Unión Europea y Argentina.

El trabajo se circunscribe temporalmente entre los años 2015 y 2020, período que permite estudiar la expansión de la aplicación de IA en los procesos sociales más cotidianos y la consolidación de los grandes monopolios en la economía digital.

Se adoptó el método de investigación bibliográfico a partir del cual se recolectó material academic y periodístico para analizar el impacto de la tecnología sobre la “sociedad en red cuya estructura social se basa en redes activadas por tecnologías de información y comunicación basadas en microelectrónica y procesadas digitalmente” (Castells, 2009, p. 51).

Hipótesis

El algoritmo permite filtrar, orientar, refinar, reutilizar y organizar grandes volúmenes de información, haciéndolos accesibles para alcanzar un resultado específico. Este proceso favorece el desarrollo de la Sociedad del Conocimiento, en permanente búsqueda de respuestas innovadoras.

Los marcos regulatorios pueden potenciar las instancias de democratización de la sociedad al promover un bienestar general con límites claros en el uso de los datos por parte de los actores que los recaban. Sin embargo, cuando los reguladores son débiles, se tiende a la

concentración en el mercado de datos y se pone en riesgo la intimidad de las personas, ya que se deja vía libre para el uso de la información de los usuarios.

Capítulo 1. “Inteligencia Artificial: Nadie sabe de mí y yo soy parte de todos”

Definiciones Iniciales

La inteligencia artificial (IA) es una disciplina que tiene impacto en áreas y sistemas complejos tan variados como vehículos autónomos, sistemas de recomendación, toma inteligente de decisiones y búsqueda en internet. Existen desarrollos de IA en asistentes personales como Alexa y Siri[2], aplicaciones médicas inteligentes de diagnóstico de enfermedades y vehículos autónomos que interpretan información del contexto e imitan las capacidades humanas de conducción (Chesñevar, Estevez, 2018, p. 127).

El término “Inteligencia Artificial” fue acuñado por primera vez en 1956 por John McCarthy, profesor de Dartmouth College que la definió como la “ciencia e ingeniería de crear computadoras inteligentes”[3].

La definición contemporánea más aceptada fue la planteada por Poole, Mackworth y Goebel en su libro “Inteligencia Computacional: acercamientos lógicos” en el año 1998. Para estos autores la IA conforma la teoría y el desarrollo de sistemas computacionales capaces de llevar a cabo tareas normalmente circunscriptas al ámbito de la inteligencia humana (p.p.146).

Los seres humanos, entendidos como agentes inteligentes, tienen la capacidad de predecir el entorno, interpretar condiciones y tomar decisiones. Las máquinas imitan las capacidades cognitivas de la mente humana, tales como la percepción visual y el reconocimiento de voz para aprender y resolver problemas progresivamente más complejos. Se genera un proceso que según Julián Siri y Juan Andrés Serur (2018), se caracteriza por:

(1) La adquisición de la información, tanto en formato estructurado (por ejemplo datos económicos), como desestructurados (imágenes y audios).

(2) Interpretación de los datos para arribar a conclusiones o conocimiento relevante.

(3) Actuar en consecuencia a partir de la comprensión de la información para completar un proceso, actividad o función definida.

4) Aprender en base al feedback (devolución o resultado) que recibe de los experimentos llevados a cabo en la vida real. Estos sistemas se adaptan y mejoran su eficacia y eficiencia a lo largo del tiempo. Esto los distingue de procesos automatizados rutinarios.

Aprendizaje Automático

[2] Servicios de reconocimiento de voz basados en la nube desarrollados por Amazon y Apple respectivamente incluidos en dispositivos móviles.

[3] http://www-formal.stanford.edu/jmc/whatisai/node1.html

El aprendizaje automático o aprendizaje automatizado (en inglés conocido como machine learning) es una de las subáreas de la IA que más evolucionó en la última década: “hace referencia a un conjunto de técnicas computacionales que permite construir modelos predictivos complejos a partir de grandes conjuntos de datos” (Chesñevar, Estevez, 2018, p. 128).

La IA representa la teoría y desarrollo de sistemas computacionales que realizan tareas que requieren de inteligencia humana. Machine learning es una metodología que se remite al diseño de una secuencia de acciones tendientes a resolver un problema (Murphy, 2013, p. 2). Este proceso es más conocido como algoritmo y se caracteriza por ser optimizado recurrentemente a través de la experiencia recolectada, aprendiendo del error, con o sin supervisión humana. El algoritmo generaliza “comportamientos” a partir de los datos de entrada: cuánto más datos, se espera que mejor sea la generalización. Los algoritmos de aprendizaje automático se modifican a partir de los datos que recibe (Bishop, 2006, p. 23).

Arthur Samuel, considerado como el padre de esta rama, afirmaba en 1959 que el aprendizaje automático es el “campo de estudio dentro de la IA que les brinda a los sistemas la capacidad de aprender de ejemplos pasados para actuar en escenarios nuevos e inciertos, sin haber sido explícitamente programados”[4].

En estos procesos se trabaja sobre bases de datos ya conocidas, a partir de las cuales se construye automáticamente un modelo predictivo que permite realizar clasificaciones y asociaciones con nueva información. Entre las técnicas de aprendizaje automático más utilizadas, que rescatan Carlos Chesñevar y Elsa Estevez (2018), se encuentran:

- **Redes neuronales:** imitan la arquitectura de redes de neuronas humanas y sus interconexiones para arribar a conclusiones, sujetas a un nivel de probabilidad. Estas redes permiten resolver problemas muy complejos, como el reconocimiento facial en una fotografía.
- **Árboles de decisión:** se elaboran automáticamente a través de algoritmos específicos y reconstruyen una serie de condiciones de recurrencia periódica para resolver un problema. Por ejemplo, muchos servicios de soporte técnico y preguntas frecuentes de plataformas utilizan esta técnica para guiar a los usuarios para resolver un inconveniente sin acudir a un contacto humano.
- **Reglas de clasificación:** permiten determinar la categoría o la clase a la que corresponde un nuevo individuo a partir de características ya conocidas. Por ejemplo, una regla que permite determinar si un cliente puede recibir un crédito analizando su salario mensual, sus créditos anteriores, conducta de pagos, su situación laboral.

[4] https://pdfs.semanticscholar.org/9330/a04e17d3b9ea092bd7dd5295b2d61d53bff5.pdf?_ga=2.97912095.1460082116.1601593385-1539072795.1601593385

- **Reglas de asociación:** descubren patrones o regularidades en una base de datos relacionando la aparición de un grupo de determinadas características con otro grupo. Un ejemplo es el caso del análisis de la cesta de compra (market basket analysis) que infiere automáticamente el patrón de compra del consumidor promedio a partir del análisis de miles de canastas de compra (si una persona normalmente compra pan y leche el sistema recomienda mermelada y manteca).

Sistemas de Recomendación: Contenidos a la carta

Los sistemas de recomendación constituyen una de las aplicaciones más extendidas de IA en las plataformas masivas.

Se trata de sistemas de filtrado de información que trabajan tomando en cuenta distintos tipos de información (películas, libros, música, noticias, imágenes, descripciones de productos, etc) que son de interés para un usuario en particular. Un sistema de recomendación "compara el perfil del usuario con algunas características de referencia y busca predecir el ranking o ponderación que el usuario le daría a un ítem que aún el sistema no ha considerado" (Scholz, Dorner, Schryen, 2017, p. 10). Estas características pueden basarse en información sobre la relación o acercamiento del usuario con el tema, su ambiente social la edad, género, hobbies, las personas con las que interactúa, las publicaciones que le gustan, sus calificaciones de productos o servicios o hasta la cantidad de tiempo que pasa en un determinado sitio web. Estos indicadores ofrecen información sobre los comportamientos que el usuario no está voluntariamente dispuesto a brindar, pero que pueden ser capturados sin intervención directa del mismo. (Marr, 2016, p. 150).

Amazon y Netflix demuestran el poder de los sistemas de recomendación. Amazon ofrece una librería personalizada para cada usuario, según sus necesidades y gustos.(Smith, Linden, 2017, p. 12). La persona que accede a su sitio de compra percibe el sitio de manera diferenciada, según sus intereses. A partir de un catálogo de cientos de millones de productos, su sistema de recomendación ofrece un reducido número de ítems de interés para el usuario. Se toma en cuenta el contexto actual y el comportamiento pasado de otros usuarios que realizaron compras con perfiles similares. Los algoritmos del sistema de recomendación construyen un modelo de patrones para construir la mejor selección de productos posibles, de forma implícita y anónima. "Amazon se dio cuenta de que las reseñas y opiniones podían hacer por él (Jeff Bezos) la parte difícil del trabajo de ventas (…) podía apoyarse en la selección y distribución" (Galloway, 2018, p. 40). Este sistema de recomendación de filtrado colaborativo se lanzó en 1998 y posibilitó una revolución en la automatización de recomendaciones para millones de clientes y con un catálogo de millones de artículos y se extendió en varios sistemas web como Youtube.

Netflix descubre los gustos de los consumidores con algoritmos y efectúa recomendaciones personalizadas. Todd Yellin, vicepresidente de innovación de Netflix, en una entrevista en la revista Wired, en agosto del 2017[5], describe el modelo de negocio de la plataforma como un banco de tres patas conformado por "los miembros de Netflix por un lado; los anotadores (taggers) que entienden todo sobre el contenido; y nuestros algoritmos de aprendizaje automatizado que toman todos los datos y hacen funcionar el conjunto como un todo". La plataforma trabaja con el concepto de perfiles para cada usuario que consume contenido en el sitio. Para cada uno de estos perfiles, se identifican los programas vistos con anterioridad y posterioridad a cada uno de ellos, la hora del día que lo hicieron y por cuánto tiempo. Eso conforma la primera pata del banco. Esta información se combina con la provista por la segunda pata: colaboradores freelance en todo el mundo que analizan cada programa de la plataforma y le asignan una anotación o etiqueta (tag) que puede hacer referencia al género al que pertenece, un actor del elenco, un sentimiento, una década, etc. "Tomamos todas estas anotaciones y los datos de comportamiento del usuario y usamos algoritmos de aprendizaje automático que infieren qué es lo más importante y cómo deberíamos examinarlo". De esta manera, se crean comunidades de gustos (taste communities), grupos de usuarios que son proclives a consumir los mismos tipos de entretenimiento.

La IA también se aplica en los chatbots (bots de charla o bots conversacional), programas de software que "simulan mantener una conversación con una persona y proveen respuestas automáticas a las consultas realizadas por los usuarios" (Chesñevar, Estevez, 2018, p. 130). Para lograr esta comunicación artificial, existen técnicas estándares de programación que seleccionan un conjunto limitado de respuestas frente a las inquietudes que reciben de las personas. Simulan reacciones y frases de un interlocutor humano con el que pueden llevar adelante una conversación con cierta lógica, a tal punto que el usuario puede no distinguir si quien le responde es una máquina o una persona. Existen distintos tipos de chatbots básicos: el informativo, el que recoge experiencias, el comercial y el de servicios (Raffath, 2016).

Datos: el nuevo petróleo

Los datos en cantidades masivas son necesarios para desarrollar y entrenar algoritmos. A través de procesos de retroalimentación, aprenden del error y aumentan su capacidad de acierto.

En los últimos años, han surgido y potenciado fuentes de datos de la más diversa naturaleza: comentarios y publicaciones, contenidos de audio y video, imágenes satelitales, datos biométricos, recibos de compra. Decantan en billones de gigabytes de nueva

[5] https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like

información producida día tras día. “Esta creciente conectividad ha acelerado la difusión de información y ha alentado la socialización del conocimiento” (Rao, 2018, p. 52).

Según lo expuesto por Luciano Galup, en su libro “Big Data y Política”, en el año 2019 sólo en 24 horas se publicaron 80 millones de fotos en Instagram, 1.000 millones de horas de video en Youtube, se enviaron 204 millones de mails y se visualizaron 10 millones de anuncios. Por minuto se realizaron 4 millones de búsquedas en Google. “Por Internet circulan 50.000 gigabytes de datos por segundo. El 90% de los datos registrados a lo largo de toda la historia de la humanidad fueron generados en apenas los últimos dos años. Para 2025 se habrán multiplicado 14 veces los datos que se produjeron hasta 2015” (2019, p. 40).

Los costos de almacenamiento caen de manera acelerada, mientras que el poder de análisis de datos crece exponencialmente (tanto desde el software como el hardware). En la industria informática tal como expone Aguiar se aplica la Ley de Moore a partir de la cual “cada año y medio, a igual precio, los chips y las computadoras que los utilizan pueden almacenar el doble de información” (2007, p. 64).

El cielo nublado de la nueva era

Galup afirma que “por primera vez en la historia la sociedad acumula más datos de los que está en condiciones de procesar y analizar” (p. 41). Esta excepcionalidad permite revertir el proceso de investigación y trabajar sobre la información ya acumulada “haciendo hablar a los datos” en lugar de tener que recabarlos como punto de partida. Lo que antes se almacenaba en gigantescas bibliotecas o infinitas cajas de archivos, ahora se resguarda en complejos entramados de servidores como Amazon o Google: lo que se conoce como “la nube”.

La nube es un dispositivo de almacenamiento global de información, disponible para el uso de cualquier usuario. La nube proviene del cloud computing definido como la prestación de un servicio de alojamiento y procesamiento masivo de datos en servidores, archivos virtuales a través de Internet. Se puede guardar todo tipo de información personal como documentos, comprobantes de pago de servicios, páginas de libros. Cualquier empresa puede llegar a alojar una aplicación de software de autoría propia en la nube de Amazon Web Services para guardar y procesar los datos. Aunque a simple vista parecen espacios de capacidad ilimitada, su mantenimiento y ampliación de espacio de almacenamiento implica una fuerte inversión por parte de las empresas dedicadas a prestar este tipo de servicio de alojamiento de información.

La infraestructura para la gestión y mantenimiento de la nube está en manos de empresas privadas (en su mayoría provenientes de Estados Unidos) o de los estados como sucede en China. Hay un tercero que almacena esa información (y que por lo tanto puede acceder y

reproducir). Los usuarios no utilizan el propio espacio de almacenamiento de su dispositivo. Estos servicios que se presentan como gratuitos tienen un costo: los datos que ceden los usuarios, registros voluntarios (publicaciones compartidas en redes, ubicaciones habilitadas o suscripciones) e involuntarios, casi invisibles como búsquedas y cookies[6].

El uso organizado de estos datos y su análisis a partir de algoritmos permiten detectar conexiones y construir patrones de comportamiento, pensamiento o consumo, idea que da lugar al surgimiento de la noción de Big Data.

Big Data

Si bien todavía el término no cuenta con una definición unívoca y consistente, sí existe un consenso respecto a las características de este nuevo fenómeno.

Los Big Data constituyen una acumulación espontánea de información. Se diferencian de otros métodos tradicionales de recolección de datos como las encuestas que tienen una estructura con objetivos predefinidos y se aplican sobre un público representativo de la muestra (Sosa Escudero, 2019, p. 31). Los Big Data son el resultado de otra acción. Por ejemplo, cuando se lee un artículo periodístico se generan metadatos: sobre qué noticias el usuario centra su interés, a qué medio acude para informarse, qué artículos sigue y hasta dónde, a qué hora del día y cuánto tiempo permanece en cada nota.

Para caracterizar el fenómeno de Big Data, Walter Sosa Escudero aplica al mecanismo de las cinco V: Volumen, Velocidad, Veracidad, Variedad y Valor:

1. **Volumen**: desde que las interacciones humanas y el consumo de bienes y servicios se llevan a cabo en la "sociedad en red" mediada por plataformas, los datos dejan de ser almacenados en formatos físicos y empiezan a ser registrados en forma automática, a través de máquinas con capacidad de almacenamiento creciente. Por lo tanto, aumenta de manera exponencial.
2. **Velocidad**: es el ritmo con el que se mueven los flujos de datos, al punto de estar disponibles en tiempo real. Las formas de consumo de cultura y de interacción entre las personas a través de plataformas exigen inmediatez como en el envío y recepción de mails o mensajes de Whatsapp. Mayor es la exigencia por la instantaneidad en eventos transmitidos en vivo en los que millones de paquetes de datos de audio y video deben llegar coordinados a millones de personas. Representa un desafío de mejora permanente de las tecnologías para expandir los límites de incorporación y circulación de datos.
3. **Veracidad**: La multiplicación de los datos da lugar a cuestionarse la calidad de la información: "el incremento de la cantidad le franquea la puerta a la inexactitud"

[6] Las cookies o galletas informáticas son pequeños conjuntos de información enviados por los sitios web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del mismo para diferenciarlos y para actuar de forma diferente y personalizada.

(Cukier Mayer-Schönberge, 2013, p.25). Implica un desafío en la recolección de los datos. Debe haber instancias de verificación de su nivel de confiabilidad para decidir si pueden ser incluidos en una investigación. Se trata de datos ruidosos y espontáneos que no se generan a partir de una base teórica ni sobre muestras definidas metodológicamente. Es la cualidad menos manejable ya que la propia lógica de la velocidad y el fácil acceso a las redes hace cuestionar la información.

4. **Variedad**: En interacción con plataformas, los usuarios generan datos diversos: tuits, fotos, archivos de texto, videos, audios, posiciones geográficas. Las sociedades compilaban su información en fuentes estructuradas como archivos públicos, expedientes, bibliotecas, agendas, álbumes de fotos. Con el desarrollo de las tecnologías, se configuró un mundo de datos desestructurados, sin formato específico. Esto permite recolectar cualquier tipo de información pero, al contar con muy poca sistematicidad, se deben idear procedimientos para organizar los datos y darles mayor coherencia.
5. La conjunción de estas cuatro características da lugar al **Valor** que adquiere toda esta información a la hora de ser interpretada. Los datos que se pueden tomar de un dispositivo móvil son muchos, pero su valor viene dado por el uso que se hace de los mismos. Por ejemplo, las ubicaciones en tiempo real de los celulares pueden ser utilizadas en aplicaciones de mapas de tránsito para detectar embotellamientos o cortes. “El valor se desplazó de las infraestructuras físicas, como la tierra y las fábricas, a los intangibles, como las marcas y la propiedad intelectual. Estos se expanden ahora a los datos (…) aunque todavía no se registran en los balances de las empresas, probablemente sea solo cuestión de tiempo” (Cukier Mayer-Schönberge, 2013, p.14).

Los Big Data son el conjunto de datos producidos de manera espontánea por la interacción de dispositivos interconectados. Se trata de datos desordenados y caóticos que pueden funcionar como fuente primaria de información si se aplican previamente técnicas de procesamiento, sistematización y estadística. Tal como puntualiza Walter Sosa Escudero “creer que la información está por el mero hecho de que los datos existen es un serio error de principiante” ya que por su naturaleza espontánea la falta de sistematización es “la regla más que la excepción” (2018, p.53).

El futuro de los Big Data radica en su masividad que puede echar luz sobre aspectos del mundo que eran inaccesibles con los métodos tradicionales. Se pueden potenciar las instancias de investigación científico-tecnológica consideradas como “una poderosa herramienta de transformación de una sociedad. La ciencia y la técnica son dinámicos

integrantes de la trama misma del desarrollo; son efecto pero también causa" (Sábato, 1993, p. 2).

Mirar los datos con cuidado

Poder aprender y generalizar a partir de los datos construye nuevas perspectivas para resolver problemas. Sin embargo, las soluciones serán tan efectivas como lo sean los datos. Si tienen sesgos, el resultado de los algoritmos se verá afectado.

Ya en 1988, se demostró que en los procesos de selección laboral, los algoritmos otorgaban puntajes menores a mujeres y candidatos de las minorías raciales. Por lo tanto, reducían sus posibilidades de ser entrevistados (Lowry, Macpherson, 1988). El problema no era que el algoritmo creara nuevos sesgos por género o raza, sino que aprendía de los datos históricos y los reproducía. Los modelos de IA actúan a partir de los datos que procesa: si los algoritmos utilizan datos que están impregnados de problemas de discriminación, los algoritmos también imitarán estos comportamientos. "Si los datos son un reflejo de la realidad tal cual es hoy, incluirán todos los prejuicios y comportamientos discriminatorios existentes en la sociedad y (…) formarán parte del algoritmo final" por ejemplo al sugerir un sueldo promedio a un posible candidato (Sampietro, Costa, 2018, p. 268).

Si el objetivo es aprender y reproducir el comportamiento humano, "los modelos de IA pueden aprender lo bueno pero también lo malo, como la acción de discriminar" (Lavista, 2018, p. 252). Estos modelos deben estar entrenados para identificar que hay discriminación y ofrecer una forma de resolverla minimizando los sesgos inherentes a los datos. Para ello, se debe controlar que los datos sean representativos, que no contengan sesgos (o tenerlos en cuenta a la hora de evaluar los resultados) y entender de qué modo el sistema identifica las características distintivas para tomar una decisión.

Deben existir instancias legales e institucionales que exijan la presencia de un equipo académico para la auditoría de los resultados. El algoritmo no puede ser una caja negra en la que confiar ciegamente: aunque los algoritmos parezcan científicos y objetivos, están impregnados de subjetividad y no son más que "opiniones embebidas en códigos" (O´Neil, 2017, p. 8). No son mejores que los seres humanos ya que están hechos a la medida de la humanidad.

Los algoritmos son en sí mismos construcciones éticas y políticas que delinean escenarios y geografías con sus propias reglas para conducir el comportamiento de millones de usuarios.

Para Lawrence Lessig el ciberespacio se encuentra regulado por cuatro tipos de limitaciones del mundo real que el autor extrapola al mundo virtual (1998, p. 172):

- La ley: Existen regulaciones en materia protección de datos, derechos de autor o de marcas que limitan los comportamientos e imponen sanciones. Con mayor o menor grado de adaptabilidad a las nuevas lógicas de funcionamiento de Internet.

- Las normas sociales: “entendimientos o expectativas de cómo uno debe comportarse” que dirigen los comportamientos de manera implícita. Por ejemplo, hay acuerdos tácitos sociales de lo que se debe/puede publicar en cada plataforma: no se sube lo mismo en LinkedIn (abocada al ámbito profesional) que en Instagram o Facebook.
- El mercado: un aumento de precio de los dispositivos o del servicio de Internet impacta sobre la cantidad de usuarios que pueden acceder a las tecnologías.
- La arquitectura: el código concebido por Lessig como “el soberano”: “el código es en sí mismo, una fuerza que impone sus propias reglas a las personas que están ahí” (1998:178). El código, como infraestructura, determina cómo los usuarios acceden y circulan en el ciberespacio: por ejemplo limita el acceso a cierta información a través de contraseñas. Encauza el comportamiento como lo hace una construcción edilicia que tiene puertas cerradas, ambientes más concurridos o espacios a los que sólo puede acceder personal autorizado.

Quien tenga el control de la arquitectura (o de los equipos que delinean la arquitectura), podrá influir en los comportamientos de millones de usuarios.

Nick Srnicek, en su libro “Capitalismo de plataformas”, hace énfasis en la “arquitectura central establecida” de las plataformas. Al ser intermediarias entre los usuarios y los prestadores de un servicio, “ganan no sólo acceso a más datos, sino además control y gobierno sobre las reglas de juego para el desarrollo de productos y servicios, al igual que las interacciones en el espacio de negocios” (2018, p. 49)

Reflexiones

Los Big Data son la nueva Biblioteca de Babel que Borges concibe como ese universo interminable de galerías hexagonales y anaqueles, ahora devenidas en grandes nubes de almacenamiento. Espacios intangibles en los que los veinticinco símbolos ortográficos que el autor reconoce se potencian y combinan en complejos lenguajes. Será labor del investigador enfrentarse a las “leguas de insensatas cacofonías, de fárragos verbales y de incoherencias”[7] de los datos de la vertiginosa y contradictoria naturaleza humana para arrojar luz sobre sus complejidades.

Detrás de la programación de algoritmos y códigos, hay cálculos propios del campo de la ingeniería que no siempre toman en cuenta criterios de las ciencias sociales para evaluar los impactos sistémicos en el conjunto de la sociedad. Se toman decisiones a diario para delinear modelos que representan una realidad a través de nuevas funcionalidades, que utilizarán millones de personas segundos después de actualizar sus dispositivos móviles. Cualquier herramienta puesta en circulación implica una apropiación social mucho más

[7] https://www.literatura.us/borges/biblioteca.html

compleja y variable que la que se pudo haber anticipado en el diseño de un algoritmo, pensado desde su funcionalidad inmediata.

¿Puede el algoritmo interpretar el lenguaje de manera equivalente al ser humano? La lengua que maneja cada sociedad va más allá que un simple conjunto de palabras con definiciones que, combinadas, permiten expresar ideas. Cada persona en interacción con los demás resignifica vocablos, expresiones, les concede una connotación especial según el contexto. Una connotación que no es inocente y que puede agredir, ofender o estigmatizar. ¿Se pueden configurar algoritmos que tengan la capacidad de interpretar el significado de los dichos humanos que circulan en Internet? Algunos hechos recientes parecen negar este interrogante. El 23 de marzo de 2016, Microsoft lanzó en Twitter a Tay, un chatbot programado para interactuar con los usuarios como una adolescente de 19 años. A través la cuenta @TayandYou[8], este bot estaba programado "para ir almacenando y procesando datos de sus conversaciones con tuiteros humanos (…) y perfeccionar su lenguaje, aptitudes y actitudes millenial para parecer cada vez más una chiquilla perfecta y más real"[9]. Sin embargo, el final no fue tan feliz: luego de 100.000 tuits, 155.000 seguidores, la cuenta de Tay fue dada de baja ya que sus respuestas se habían vuelto misógicas, racistas y xenófobas en sólo 16 horas de vida. Microsoft explicó que se trató de un hackeo y prometió volver a lanzar este desarrollo de Inteligencia Artificial corregido, aunque hasta el 2020 aún no ha revivido en el mundo de los 140 caracteres. El jefe de investigación de la empresa, Peter Lee, atribuyó estos comportamientos a un ataque coordinado de trolls[10] que, a través de patrones de conducta repetitivos en las respuestas, influyeron en las capacidades conversacionales de Tay. Nunca se pudo dar una explicación clara de por qué el bot llegó a publicar twits antifeministas, de contenido sexual, trató a Barack Obama de "mono" y desmintió el Holocausto[11].

El 7 de agosto de 2020, Cristina Fernández de Kirchner presentó una denuncia a Google debido a que el día 17 de mayo, si se introducía el nombre de la Ex Presidenta, el buscador incluía en su panel de conocimiento su foto junto a la leyenda "Ladrona de la Nación Argentina". El panel de conocimiento es un recuadro que aparece por encima de los resultados, a la derecha de la pantalla y su contenido se define automáticamente por un algoritmo que presenta datos mayormente reconocidos. En este espacio, se ofrece un resumen sobre un tema específico, basado en la interpretación que Google hace de los contenidos relacionados disponibles en la web. Los contenidos se actualizan de manera automática a medida que cambia la información de múltiples fuentes. Tal como ejemplifica

[8] https://twitter.com/tayandyou
[9] https://www.publico.es/ciencias/inteligencia-artificial-internet-tay-robot-microsoft-nazi-machista.html
[10] Un troll es una cuenta, anónima o no, que publica mensajes agresivos, violentos o despectivos con el objetivo de molestar a las comunidades digitales, desviar la conversación o bloquear (Galup, 2019, p. 156).
[11] https://archive.org/details/taytweets

Henoch Aguiar en una entrevista en el programa de radio “Porque” de Graciela Fernandez Meijide[12] en agosto del 2020, si se define una persona como capitana de un equipo de fútbol y se la busca en Google, aparecerá en el panel de conocimiento su nombre con el título “Capitán del equipo X”. Podría ocurrir que luego de varios partidos, el capitán no tuviera un buen rendimiento en la cancha, por lo que muchos usuarios en la web lo tildarían de “tronco”, una expresión muy común en la jerga argentina para hacer referencia a los malos jugadores. Si en un momento determinado, el algoritmo de Google que define el panel de conocimiento identifica que los contenidos en contra de la performance del capitán son superiores a su puesto dentro del equipo, puede llegar a mostrar “tronco” en lugar de “capitán” al ingresar su nombre en el motor de búsqueda. ¿Por qué sucede esto? Si se analiza la gramática de las palabras, “tronco” es un sustantivo tal como “capitán”. El problema es que en Argentina utilizar “tronco” tiene una connotación de adjetivo, se le asigna una cualidad a la persona. Para el algoritmo ambas palabras son sustantivos y se basa en el número de veces que aparece cada palabra en la web para definir lo que muestra en el buscador. ¿Es tonto el algoritmo?, ¿se puede decir que comete un error?, ¿hay forma de indicarle al algoritmo cómo interpretar cada palabra según los contextos socials y significados compartidos colectivamente? Más allá de todos estos interrogantes, el hecho de que el nombre de una persona aparezca ante millones de usuarios asociado a ciertas expresiones, puede tener impacto en la vida real.. Estos “incidentes” comienzan a circular viralmente en la web y tienen miles o millones de réplicas en las redes. ¿Se puede dejar el manejo de la información sólo en manos de algoritmos?

Cualquier error de cálculo, cualquier falla o vulnerabilidad de un sistema impacta en la vida de las personas. No existe un mundo digital escindido de las condiciones materiales de la sociedad. Una sociedad más diversa y heterogénea. Los procesos de estandarización y repetición de los algoritmos ¿contemplan esta diversidad?, ¿se pueden construir variables o categorías de identidades, de ideas políticas, de valores?, ¿quién define esas variables?, ¿los equipos de desarrollo de las empresas son representativos de los públicos a los que apuntan?

¿Puede un algoritmo decidir si se le otorga un crédito a una familia para financiar una intervención médica? Los sistemas tienen una admirable capacidad predictiva pero hay elementos intrínsecamente humanos que no pueden maquetarse en una fórmula: la empatía, la racionalidad, la emocionalidad.

12 https://soundcloud.com/henoch-aguiar/2020-08-16-porque-aguiar

¿Qué consecuencias puede tener dejar todo librado a las decisiones automáticas? Las matemáticas y los sistemas se consideran fuentes confiables sin intencionalidad. No se equivocan, no se distraen, no se dejan llevar por las emociones, no se cansan, pueden evaluar múltiples variables, no envejecen como el cerebro humano. Procesan vastas cantidades de datos mucho más rápido y objetivamente que los seres humanos y, por lo tanto, pueden tomar decisiones mucho más responsables. Esta idea se conoce como Mathswashing: considerar a las decisiones automáticas mejores y más eficientes, apoyándose en la idea de objetividad implícita en las ciencias duras.

¿Existen instancias de auditoría para clarificar los procesos de decisión o están protegidos por la propiedad intelectual de aquellos que configuraron los algoritmos?, ¿qué pasa si un algoritmo toma una decisión que puede ser interpretada como discriminatoria?, ¿se le puede echar la culpa?, ¿quién es el responsable de un error?

Se debe acentuar y exigir el trabajo de personas del campo de las ciencias sociales para plantear debates éticos, definir cursos de acción frente a escenarios particulares, analizar los resultados. Estos actores deben ser mediadores entre el programa y la sociedad para traducir y hacer inteligibles los procesos automáticos. Por ejemplo, si una plataforma educativa debe calcular el promedio de un alumno, toma sus calificaciones y hace el cálculo correspondiente, pero ¿qué pasa si ese alumno experimenta circunstancias particulares en su vida personal o en su proceso de aprendizaje?, ¿se le pueden indicar este escenario a los algoritmos? Si es así, ¿quién tiene acceso a esa información sensible?

Se invirtieron los procesos de investigación ya que los datos están disponibles antes de iniciar el proceso de recolección gracias a herramientas como Big Data. Al hablar de Big Data, ¿se puede hablar de todos los datos?, ¿esos datos son representativos de una muestra bajo técnicas como las que se aplican en la estadística? La información que las personas generan sobre sí mismas en su interacción con plataformas no es exacta y, sobre todo, es incompleta. El hecho de que existan profundas desigualdades en el acceso a las tecnologías, implica también que haya sectores de la sociedad que no estén representados en los conjuntos de datos.

Los algoritmos definen perfiles digitales que determinan filtros y sistemas de recomendación sobre los contenidos a los que acceden los usuarios. Deben llevarse a cabo investigaciones desde el campo de las ciencias sociales que rescaten conceptos teóricos de otros contextos históricos y los resignifiquen bajo la óptica de las nuevas tecnologías: “el interesante enigma de nuestros tiempos es que caminamos sonámbulos de buen grado a través del proceso de reconstrucción de las condiciones de la existencia humana” (Winner, 2008, p.43).

Desde la comunicación, se puede retomar el concepto de la Aguja Hipodérmica desarrollado por Harold Laswell en el período de entreguerras entre las décadas de 1920 y 1930. Encuadrado en el funcionalismo, se abocó al estudio de los fenómenos de

propaganda y el potencial poder de persuasión de la comunicación de los medios masivos de la época. Tomó en cuenta los supuestos del conductismo que se basan en la lógica de estímulo y respuesta: frente a determinado estímulo, existen ciertas funciones básicas biológicas que pueden ser condicionadas para actuar de una determinada manera. Aplicándolo al funcionamiento de los medios, Laswell concluyó que un mensaje puede reunir condiciones específicas que son capaces de penetrar en la mente de los receptores y conducir su acción. Esta teoría fue fuertemente cuestionada y desestimada bajo el argumento de que la construcción de sentido es social y las personas interpretan los mensajes de diferente manera según sus contextos y la interacción con otros.

En su ensayo "Teoría de la propaganda política" del año 1927, Laswell estudió el fenómeno de propaganda e interpelación y argumentó que "una mirada a los patrones de vida de cualquier comunidad revela la red de rutas de movilidad y centros de congregación a través de los cuales hechos y opiniones interesadas pueden diseminarse" (1927, p 630). ¿Qué opinaría Laswell de los algoritmos que definen las estrategias más atractivas para captar la atención de los usuarios basándose en el conocimiento preciso de los patrones de consumo?, ¿hasta qué punto un algoritmo puede conducir las conductas para lograr por ejemplo, que se compre un producto? Aún más, ¿qué pasa si se considera que el usuario en sus redes interactúa con públicos que simpatizan con los propios ideales?, ¿qué tipo de reinterpretación puede hacerse de los mensajes?, ¿se puede hablar de nuevas "agujas hipodérmicas digitales?[13] Tal como argumenta Byung-Chul Han "la interconexión digital total y la comunicación total no facilitan el encuentro con otros. Más bien sirven para encontrar personas iguales (…) haciéndonos pasar de largo ante los desconocidos (…) y se encargan de que nuestro horizonte de experiencias se vuelva cada vez más estrecho (2017, p. 12)

[13] https://www.ambito.com/opiniones/redes-sociales/agujas-hipodermicas-digitales-n5140120

Capítulo 2: “Estados alterados”

Datos en la burocracia estatal

En lo que va de este siglo, la gran mayoría de los Estados transitan hacia un modelo burocrático digital basado en cuatro grandes grupos de acciones: modificación de la gestión documental y de los expedientes hacia formatos electrónicos o digitales; diseño e implementación de sistemas de gestión basados en plataformas digitales; trámites a distancia y servicios digitales; cambios en la organización administrativa (Corvalán, 2018, p. 259).

Herrero y Gentile plantean que “la transparencia, el acceso a la información gubernamental, la rendición de cuentas y la participación social en los asuntos públicos, así como la amplia utilización de las tecnologías de la información” son pilares fundamentales para lograr generar “gobiernos más eficientes y abiertos y por ende con mayores niveles de rendición de cuentas” (2012:02).

El uso de canales digitales impacta en la relación con el Estado y sus dependencias. Según un estudio realizado en Junio de 2018 por Latinobarómetro[14], una Corporación sin fines de lucro de Chile, en América Latina el promedio de horas para completar un trámite es de 5.4 horas considerando “tomar el bus, hacer fila, esperar en ventanilla, leer un aviso, llenar un formulario, mandar una carta o incluso aprender a utilizar una página web”. Si existe la posibilidad de iniciar o hacer seguimiento de un trámite por vías digitales, se reduce el tiempo que el ciudadano le dedica a los procesos burocráticos y esto impacta directamente en su calidad de vida. Hablar de un Gobierno Electrónico implica según Darío Laufer en la Carta Iberoamericana del Gobierno Electrónico “mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector y a participación de los ciudadanos” (2009, p. 2). Sin embargo, hablar de transparencia y participación ciudadana no son sinónimos. Los estados pueden hacer uso de las nuevas tecnologías para modernizar los procesos internos sin que eso signifique crear los espacios que exige la figura del ciudadano en tanto soberano y mandante. El modelo público no es una consecuencia natural de la modernización y cambios tecnológicos.

Este tipo de proyectos puede generar resistencias entre el personal abocado a las formas de trabajo tradicionales ya que se percibe como un avance sobre sus tareas. Por el contrario, el objetivo es automatizar procedimientos burocráticos y repetitivos para destinar más tiempo a tareas que requieran de la sensibilidad e imaginación propiamente humanas que pueden agregar valor a las decisiones.

[14] https://medium.com/@carlos_pared/tr%C3%A1mite-un-mal-necesario-b438022fc66f

El Estado, según Prince, tiene un triple rol en su relación con las Tecnologías de la Información y la Comunicación: por un lado, el Estado es "dador del marco normativo y regulatorio general y específico, y de las condiciones sociopolíticas y económicas estructurales adecuadas"; por otro lado, es "promotor y catalizador de la iniciativa privada a través de lineamientos, políticas y programas claros y eficaces para todos los actores involucrados, en busca del desarrollo local y adopción de estas tecnologías"; y por último, es el "usuario modelo y principal, tanto en la administración como en el gobierno" (2002:01). En los últimos años, podría hablarse de una reconversión de esa última relación, ya que la masificación y apropiación del uso de las nuevas tecnologías por parte de la ciudadanía hace que la tecnología deje de ser Estado-céntrica para pasar a ser ciudadano-céntrica. Esto implica que los Estados deben observar constantemente los procesos de significación de los espacios virtuales y herramientas digitales para no perder de vista las dinámicas de funcionamiento social.

Un sector público inteligente presupone adoptar un paradigma de inteligencia híbrida que combine inteligencia humana con IA como lo es el caso de Prometea en Argentina, un sistema de IA que funciona en el Ministerio Público Fiscal. El proyecto surgió gracias al trabajo conjunto de los abogados Luis Cevasco y Juan Corvalán con programadores especializados. El objetivo, en palabras de Corvalán (Co Director del Laboratorio de Innovación e Inteligencia Artificial de la Facultad de Derecho de la UBA), fue "terminar con la injusticia de que un mismo ciudadano, con el mismo problema, recibiera dos respuestas diferentes por parte del Estado".[15]

Este sistema no aprende derecho en el sentido humano, pero cuenta con la capacidad de leer, predecir, escribir y resolver un expediente judicial en un promedio de 20 segundos con una tasa de acierto del 93%. Prometea resuelve alrededor del 52% de los casos en materia de derecho a la vivienda, al trabajo y cuestiones de remuneraciones de empleados públicos que llegan a la Fiscalía General Adjunta en lo Contencioso Administrativo y Tributario de la Ciudad Autónoma de Buenos Aires. Interactúa con el usuario como un chatbot conversacional que lee, comprende y contrasta los casos históricos para encontrar ante un nuevo expediente patrones comunes en las resoluciones previas. Corvalán afirma: "Para nosotros, la IA humaniza porque ahora tenemos una oportunidad de salir de la costumbre, y que la máquina resuelva lo que es meramente estadístico, mientras que nosotros ponemos nuestro trabajo en casos que merecen toda nuestra atención, y generamos empatía con el ciudadano".

Ciudadanía y Tecnología

[15] https://www.ambito.com/politica/justicia/prometea-inteligencia-artificial-hacer-n5061091

Para construir un ecosistema de tecnologías disruptivas de la 4º Revolución Industrial al servicio de la sociedad, debe haber políticas de educación y alfabetización digital tanto en la ciudadanía como en el sector público. Si el ciudadano entabla diálogo con los gobiernos mediante el uso de aplicaciones, Inteligencia Artificial y herramientas como Big Data sobre los datos que genera, hay que repensar la forma en la que la sociedad se expresa para poder sostener un diálogo ciudadano, inteligente y humano. La autora Levy Daniel concede a Internet "un gran potencial para permitir a las personas expresarse, participar en las discusiones públicas, así como acceder a bienes y servicios, lo que fomenta los principios básicos de una sociedad democrática." (2016, p 11). La "sociedad en red" definida anteriormente ha devenido esencial en el ejercicio de derechos fundamentales.

Internet abrió nuevos espacios de conversación, relación y acción política en los que los gobiernos pueden participar para conocer los intereses y preocupaciones de los ciudadanos. "Construir puentes con demandas fragmentadas, con preocupaciones que no tienen grandes representaciones, pueden ser una forma de empezar a reducir la brecha con una ciudadanía desencantada" (Galup, 2019, p.92). Las redes se suman al debate público a partir del activismo de la ciudadanía. Sin embargo, cabe considerar que la vida en redes sociales también implica nuevas y múltiples formas de censura, a veces, desde la propia gestión de los contenidos por parte de las propias empresas detrás de aquellas redes. No son pocos los casos de recorte o bloqueo de imágenes sin un criterio íntegramente definido. Por eso, es necesario cuestionar la presunta libertad de expresión potenciadora de las redes.

El proyecto "Map Kibera: Making the Invisible Visible"[16] es un claro ejemplo: a través de la participación ciudadana y la tecnología, se incorporó a Kibera, un barrio de Nairobi, en mapas colaborativos. Este barrio no existía en ningún tipo de cartografía. Como sus habitantes utilizaban locutorios, los responsables del proyecto los rastrearon digitalmente y los incluyeron en mapas a través del uso de diferentes programas y recursos online, entre ellos OpenStreetMap[17] (un sitio web que permite acceder gratuitamente a un mapa mundial colaborativo y de uso libre bajo licencia abierta). A partir de que Kibera comenzó a aparecer en mapas colaborativos como Wikipedia, aunque no estuviera en representaciones oficiales, sus habitantes pudieron reclamar servicios esenciales como agua potable.

Otro caso de uso de los datos generados por la misma ciudadanía es la herramienta "Mapa de Oportunidades Comerciales (MOC)"[18] desarrollada por el Gobierno de la Ciudad de Buenos Aires y Telefónica. Con la tecnología Smart Mobility que procesa los datos agregados de los flujos urbanos de movimiento, se puede consultar para una determinada dirección y rubro la cantidad de gente que transita por ese punto, las líneas de colectivo y

[16] https://mapkibera.org/
[17] https://www.openstreetmap.org/#map=4/-40.44/-63.59
[18] https://www.buenosaires.gob.ar/empresas/planifica-tu-emprendimiento/elegi-tu-local/mapa-de-oportunidades-comerciales

otros medios de transporte en las cercanías, si existieron picos de apertura o cierre de locales, si en esa dirección exacta ya hubo un comercio del mismo rubro y explorar los rubros con más y menos riesgos. Así, un ciudadano puede evaluar las variables de una determinada locación a la hora de instalar un comercio en un determinado punto de la ciudad.

Caso Estonia

Un caso paradigmático en la digitalización de los procesos de gobierno es el de Estonia, ubicado en el noreste de Europa y parte de la Unión Europea desde el año 2004.

Este país desarrolló el primer e-gobierno del mundo. Desde su independencia reemplazó el papel por un sistema de bases de datos conectado a Internet que permite conocer online y en tiempo real datos como los gastos del estado.

En el año 2019, fue catalogado como el país "más digital del mundo" ya que todos los trámites se pueden hacer online salvo el casamiento, el divorcio y la transferencia de propiedades. En promedio, cada ciudadano estonio ahorra dos semanas por año al simplificar los canales para la realización de trámites.

El principio rector del sistema de Gobierno Electrónico es el "Once only": se almacena la información del ciudadano de manera tal que no se le solicita el reingreso de sus datos personales cada vez que necesita hacer un trámite. Esto se logra gracias a la interoperabilidad y comunicación entre todas las dependencias del estado.

El 98% de los ciudadanos tienen un ID digital único, obligatorio y universal de 11 dígitos que se implementó en el año 2002 (en la mayoría de los países este tipo de identificación digital es opcional). Este Id se le asigna a cada ciudadano al nacer, y lo acompaña a lo largo de toda su vida en todas las instancias de participación ciudadana: desde el ejercicio del voto (en el 2019, el 46,7% de los ciudadanos votó por medios electrónicos y el resto lo hizo en papel por decisión propia) hasta el acceso a más de 4 mil servicios digitales como declaración de impuestos, registro de un negocio, renovación de la licencia de conducir, acceso a historiales médicos online y prescripción electrónica de recetas por correo electrónico.

Esta identificación está conformada por un documento de identidad que contiene un chip y un cifrado especial de clave pública (denominado ECC o Elliptic Curve Cryptography).

Para garantizar la seguridad, la información se aloja en una arquitectura distribuida denominada X-road, en lugar de un servidor centralizado. En caso de que se produzca un ciberataque, no se podrán vulnerar la totalidad de los datos de la ciudadanía. Cuenta con una protección de Blockchain o cadena de bloques definida como un "registro único, consensuado y distribuido en varios nodos de una red"[19]. Cada bloque cumple con una

[19] https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/

función específica e inalterable dentro de la cadena que conforma una red descentralizada y, por lo tanto, muy difícil de hackear.

El país cuenta con copias de seguridad de los datos originales (backups), creó la primera embajada de data en Luxemburgo y aplica métodos de verificación en dos pasos para garantizar la identidad de los usuarios. Estas medidas de extrema seguridad se tomaron luego de que en 2007 sufrieran un ciberataque ruso a sus sistemas por motivos políticos.

Estonia ocupó los primeros puestos en Europa como el país con mayor penetración de Internet y telefonía móvil. En el año 2013, el 95% de su territorio ya estaba cubierto por la tecnología 4G. Se trata de la primera nación que declaró Internet como un "derecho humano básico".

Marten Kaevats, asesor digital del gobierno de Estonia afirma que "la digitalización no pasa sólo por la tecnología, sino por cambiar la mentalidad de la gente (..) de papel a digital"[20]. Para lograrlo, el país se centró íntegramente en la educación. En 1996, se implementó "Tiigrihüpe" (el Salto del Tigre), un programa de modernización tecnológica cuyo objetivo era lograr el acceso a computadoras conectadas a internet en las escuelas acompañado por la enseñanza de uso de herramientas informáticas[21]. En un año, el 40% del personal docente adquirió conocimientos avanzados sobre informática y programación a través de capacitaciones y hasta el 98% de las escuelas contaron con acceso a Internet. Además, se distribuyeron más de 100 programas de software educativo y se creó un sitio web colaborativo con material didáctico para profesores. Los planes de estudios de las escuelas, desde el jardín de infantes, incluyen la enseñanza de programación.

Las instituciones educativas fuera del horario escolar, abrieron sus puertas al resto de la comunidad para que accediera a la tecnología y aprendiera computación. Entre los años 2002 y 2004, se dictaron cursos de informática para adultos a través del programa Vaata Maailma ("Una Mirada al Mundo")[22] financiados por el sector privado. Este proyecto se transformó en una Fundación que, entre 2011 y 2012, brindó un programa de entrenamiento en tecnologías de la información (IT) a personas desempleadas. La idea era que pudieran reubicarse en el mercado laboral de la industria de la tecnología nacional ya que por su baja densidad de población, el país contaba con una profunda escasez de personal especializado.

En el plano económico, el gobierno incentiva la creación y desarrollo de StarUps. Este tipo de políticas se iniciaron luego de Microsoft le comprara al país por un valor de USD 8.500 el software que permitió la creación de Skype, la plataforma de videollamada en tiempo real a través de Internet. Los fondos recibidos se invirtieron en nuevas StarUps combinadas con

[20] https://www.infobae.com/tecno/2019/11/20/como-estonia-se-convirtio-en-el-pais-mas-digital-del-mundo/
[21] https://eldefinido.cl/actualidad/mundo/5143/De-ruina-postsovietica-a-potencia-Asi-lo-hizo-Estonia/
[22] https://ec.europa.eu/budget/euprojects/foundation-vaata-maailma_en

inversiones extranjeras que comenzaron a prestar atención en los desarrollos de la nación. En el año 2019, fue el país con mayor cantidad de StarUps per cápita del mundo.

Estonia es un claro ejemplo de que la voluntad política y el trabajo con el sector privado y la sociedad civil pueden estimular el desarrollo del conocimiento y tecnología y así impulsar el crecimiento de una sociedad en su conjunto. Se trata de uno de los países más pequeños del mundo que cuenta con sólo 1.3 millones de habitantes. Con una agenda digital consistente y actualizada, Estonia es a nivel mundial un modelo a seguir en materia de implementación de Inteligencia Artificial en los procesos del estado, en pos del bienestar de la sociedad.

Reflexiones

Los gobiernos deben implementar y profundizar políticas de datos abiertos para poner la tecnología a disposición del ciudadano. ¿Qué implica hablar de datos abiertos? Abrir y crear canales de bases de datos de fácil acceso, sin ningún tipo de restricción en la distribución, con información desagregada en los formatos más ampliamente utilizados y familiares para la ciudadanía. Este factor permite abogar por un mayor grado de transparencia por parte de las dependencias públicas ya que la sociedad puede acceder fácilmente a la información para hacer una apropiación y análisis personal al hacerlos dialogar e interactuar, sin depender de análisis o variables previamente definidas.

El personal del sector público debe contar con tecnologías de hardware y software lo suficientemente preparadas y modernas para la carga de información. Las infraestructuras de seguridad deben ser confiables y mantenerse actualizadas ya que los datos que pueden recabarse de los ciudadanos pueden ser extremadamente sensibles. Un expediente judicial puede ser almacenado en la cuenta personal de un empleado en lugar de utilizar las bases propias del Estado por no contar con la capacidad de almacenamiento. De esta manera, no hay forma de asegurar que ese usuario aplique las mismas medidas de seguridad presentes en los sistemas públicos, ni tampoco está exento de ser hackeado.

El personal público debe contar con las competencias necesarias para trabajar con herramientas de procesamiento de datos. Deben definirse lineamientos comunes en los formatos en los que la información es almacenada e implementarse plataformas comunes e interoperables. Si no se cuentan con bases de datos comunes y colaborativas, se lentifican los procesos ya que el ciudadano por ejemplo debe cargar la misma información personal cada vez que inicia un trámite. Mientras el trámite está en proceso, se puede obstaculizar su avance debido a que una dependencia solicita información a otra y debe esperar que su pedido se procese, se recabe y sea enviado a su propia base.

Es importante hacer una buena lectura de los contextos ya que de lo contrario, pueden existir canales alternativos pero el ciudadano preferirá los caminos tradicionales. En el caso

de un trámite, puede optar por gestionarlo físicamente porque no está familiarizado con los dispositivos, no cuenta con buena conectividad o porque simplemente desconfía del carácter intangible de la información.

Los ciudadanos, desde su propia experiencia, pueden aportar evidencias y visibilizar problemáticas. Primero, deben contar con los canales para hacer llegar su experiencia y acceder a los datos de otros contextos para hacer una apropiación novedosa, y tal vez impensada, de lo que superficialmente puede verse como información desagregada.

Debe existir una genuina voluntad política para resignificar el lugar del ciudadano: no basta con cargar bases de datos en sitios web oficiales sino que se trata de un proceso muchísimo más integral. Tal como sucede en Estonia, desde los primeros años de la formación educativa se enseñan conocimientos que permiten comprender los nuevos entornos digitales y las herramientas para poder trabajar en sus propios proyectos. El Estado debe garantizar la conectividad de la ciudadanía en su conjunto y tener también protocolos y personal abocado para responder a las necesidades que los ciudadanos hacen llegar a través de los nuevos canales digitales.

Se deben delinear políticas que tengan continuidad más allá del signo político del gobierno de turno. De nada sirve invertir recursos para crear plataformas o servicios de datos públicos que luego quedarán desactualizadas o sin mantenimiento. El mundo digital es, ante todo, efímero y poco claro a la hora de ser gestionado. Un cambio de política de un gobierno a otro, puede implicar que ciertos datos abiertos sean eliminados o inhabilitados de las bases públicas sin que quede un registro de ello.

Siempre es una buena noticia la apertura de nuevos sitios web públicos de participación ciudadana que abogan por la transparencia. Pero si no hay una lectura, un tratamiento y análisis posterior por parte del Estado, el ciudadano seguirá hablando con un contestador automático, escuchando música de espera.

La Inteligencia Artificial potencia el poder de aquellos que se valen de ella para resignificar actividades y procesos. Las nuevas tecnologías en manos del Estado maximizan su capacidad de control para avasallar al ciudadano y hacer un seguimiento mucho más acabado del mismo. ¿Se puede aplicar la IA para distribuir el poder en lugar de coartar los derechos y libertades de la ciudadanía? La tecnología debe estar también al servicio de la ciudadanía para empoderarla al crear los espacios que le permitan defender esos derechos y libertades. No se trata sólo de tener canales virtuales para hacer trámites más rápido, porque eso también implica más control y registro de todos sus datos en plataformas de dependencias públicas. Entrenar a los ciudadanos con competencias digitales debe ser el primer paso para reforzar las capacidades de la sociedad y para entablar un diálogo directo con el Estado. Acceder a datos abiertos actualizados de la información pública le concede al ciudadano la posibilidad de conocer, evaluar y denunciar cualquier irregularidad que

detecte. Los ciudadanos cuentan con su experiencia diaria, su visión acabada de los hechos y problemáticas que lo rodean a nivel local, provincial, nacional. Tienen mucho que aportar a los procesos de debate de políticas públicas. Sin embargo, si el Estado se consolida como un panóptico omnipresente que todo lo ve, la sociedad tenderá a estar cada vez más cercenada en un mundo en el que la digitalización de la vida ya es inevitable.

Lo importante no es lo digital en sí mismo sino todo lo humano que lo digital viene a resolver. El ciudadano es el actor que más cerca está de sus propias problemáticas y que, por lo tanto, puede aportar la visión más acabada de sus experiencias como protagonista. El Estado debería implementar la Inteligencia Artificial como una herramienta que haga posible conectar las preocupaciones, ideas, problemas, interrogantes de los ciudadanos con aquellos profesionales formados para encauzar soluciones relevantes, más allá de las distancias que los separen. El objetivo es fortalecer una conexión dinámica entre el conocimiento especializado y las problemáticas de la sociedad, de manera tal que las respuestas lleguen de la forma más rápida y efectiva posible. Sólo en ese camino, la Inteligencia Artificial será un vehículo que potencie a la ciudadanía como parte de la tripulación que direccione las políticas de los estados.

Capítulo 3: “La mirada (in)discreta”

Luego de la Segunda Guerra Mundial, las disciplinas y los grandes sitios de encierro se sumieron en una profunda crisis. Las sociedades disciplinarias, con sus dispositivos, mecanismos y espacios, dieron paso a las sociedades de control.

El control, a partir de esta nueva categoría de sociedades, trasciende los lugares de encierro. Se ejerce de manera segmentada desde cada dispositivo que las personas llevan consigo tanto en el ámbito público como en su propia intimidad: “el panóptico de Jeremy Bentham se concretiza hoy en día en una “sociedad de cristal” resultante del infinito proceso de retroalimentación de datos, la informática y las telecomunicaciones” (Guida, Himelfarb, Sanchez Porto, 2009, p.2). Se conforma un modelo más opresivo que el de las sociedades disciplinarias ya que antes había posibilidad de escape en el espacio público. En las sociedades de control hay una continuidad del encierro mediante la tecnología, tal como argumenta Castells “Internet se consolida como instrumento esencial de la expresión, información y comunicación horizontal (...) la red no se controla, pero sus usuarios están expuestos a un control potencial de todos sus actos más que nunca en la historia” (2001, p. 7). Se trata de un control que ya no tiene fronteras entre adentro y afuera y son los propios usuarios en su interacción en redes los que “se entregan voluntariamente a la mirada panóptica. (…) El morador del panóptico digital es víctima y actor a la vez” (Byun-Chul Han, 2013, p 51).

Nuevas Sociedades de control: China

“La Muralla Digital China” conforma un sistema de “espionaje masivo” a través de la red más extensa de cámaras de reconocimiento facial del mundo.

En 1987, en un laboratorio de Pekín, se envió el primer correo electrónico chino que decía “Más allá de la Gran Muralla, podemos llegar a cualquier rincón del mundo”. El desarrollo de Internet le permitió atravesar la gran muralla de las dinastías imperiales y vincularse con el resto del mundo. Pero el Partido Comunista de China rápidamente construyó una nueva muralla: La Muralla Digital. Gran parte de la vigilancia pasa a ser una cuestión digital que empuja tanto a las plataformas como a los usuarios a autocensurarse por temor a ser sancionados.

China cuenta con más de 800 millones de usuarios en Internet, pero no es la misma red que actúa en Occidente. Tanto Google como Facebook están bloqueados, y la industria se encuentra dominada por 3 gigantes nacionales: Baidú (buscador, el Google chino), Alibaba (plataforma de comercio en línea) y Tencent (red social al estilo de Facebook). Este trinomio, conocido como BAT, se encuentra por encima del grupo GAFA (Google, Apple, Facebook, Amazon). En lugar de Whatsapp, se utiliza la plataforma de comunicación

instantánea WeChat que tiene más de 1000 millones de usuarios activos al mes. Esta aplicación de mensajería puede impedir, mediante el uso de algoritmos, la transmisión de fotos en tiempo real. Cuando se envía un contenido, este se coteja con bases de datos y, si resulta sospechoso, el envío se bloquea.

El país cuenta con 176 millones de cámaras de seguridad, 1 cada 8 personas. La policía utiliza gafas con un sistema de algoritmos que comparan los rasgos de una cara con las imágenes almacenadas en las bases de datos. Para ello, se apoyan y sustentan en la base de datos “Sky Net” que permite reconocer en segundos a un individuo entre su vasta población. Aplican el sistema Dragonfly Eye System, desarrollado por la empresa de inteligencia artificial Yitu que declara ser capaz de detectar y reconocer al instante una cara entre 2.000 millones de personas con una exactitud del 95,5 por ciento. Se basan en un fuerte componente tecnológico para generar terror en la población.

A principios del 2018, China implementó el programa piloto “Ojos Agudos”, que busca conformar una plataforma nacional de vigilancia y datos compartidos a partir del cruce de información entre cámaras de reconocimiento facial en espacios públicos, edificios privados y complejos habitacionales. Todos estos datos se almacenan en una “nube policial” que los clasifica en categorías como compras online, archivos criminales, reservas de viajes, archivos médicos y los vincula con el documento de identidad y el rostro de cada persona.

Se trata de un entramado de artefactos digitales interconectados que generan datos y se entrecruzan de manera tal que el individuo es vigilado y evaluado permanente.

Los datos biométricos obtenidos de los ciudadanos se recopilan a través de la instalación de domos y cámaras de drones que sobrevuelan las ciudades. Esa información se vincula con las compras que los ciudadanos hacen en Aliplay, sus conversaciones en WeChat, los viajes en transporte público y las multas por infracción, por citar sólo algunos de los ejes que se relación en segundos. Todas las bases de datos están bajo el control del Partido Comunista Chino.

Este estado de vigilancia gamificado, tal como se lo conoce en el resto del mundo, comenzó a aplicar a partir del 2020 el Sistema de Crédito Social (SCS), basado en un mecanismo de premios y castigos. El Estado asigna a cada ciudadano un puntaje basado en su conductas (con quién interactúa, qué busca en Internet, qué productos compra). Los datos se unifican en una plataforma nacional en manos del Estado para ejercer control sobre la población. Por ejemplo, aquellas personas que viajan en tren sin boleto, obtienen bajas calificaciones o no pagan las cuentas a tiempo, bajan su puntaje. Esto impacta en la vida real de los ciudadanos que son sancionados: pueden estar inhabilitados para recibir atención médica en ciertos centros de salud, comprar autos de alta gama, viajar en transporte público o acceder a matrículas en determinadas instituciones académicas o préstamos en bancos.

En China, existen proveedores locales para todos los servicios que ofrece Internet occidental. Esto hace que todo el tráfico de información del país, pase por esos pocos servidores. Así, gobierno chino bloquea fácilmente contenidos y rastrea permanentemente la actividad de los ciudadanos en la red. En este sistema, las empresas chinas no compiten con los gigantes extranjeros, ya que la mayoría de estas plataformas se encuentran bloqueadas.

La situación más extrema se da en la región de Xinjiang (noroeste de China), donde habitan los uigures (minoría musulmana) y otras pequeñas etnias. Allí se creó la "Plataforma Integrada para Operaciones Conjuntas" que recopila datos personales (como fe religiosa, grupo sanguíneo, licencia de conducir, profesión, patrones de movilidad) y etiqueta a las personas sospechosas como peligrosas. Los extranjeros que ingresan a esta región por tierra deben entregar sus celulares a los guardias fronterizos para que les instalen una aplicación que analiza contactos, videos y mensajes de voz a partir de 73.000 criterios de búsqueda diferentes.

¿Cómo es posible configurar un sistema de control tan específico? Todo el tráfico de datos de China está aislado del resto del mundo digital por un enorme "cortafuegos informático" o firewall: "La Muralla Digital China", "La Gran Muralla de Fuego" o "El Escudo Dorado de China" que bloquea el acceso a la información. Permite conocer con nombre y apellido quién navega por Internet, qué hace allí, con quién se contacta y cuáles son sus intenciones.

El Gran Cortafuegos

La plataforma de investigación periodística Initium, con sede en Hong Kong, realizó un informe sobre la evolución del Gran Cortafuegos y de las herramientas que se utilizan para eludirlo. Este es el resumen traducido por globalvoices.org que definió cuatro fases del desarrollo de esta tecnología de bloqueo:

- En su etapa inicial, el Escudo Dorado bloqueó nombres de dominio y direcciones IP. Se podía evitar con el uso de un servidor extranjero.
- En una segunda fase, se optimizó el Escudo para poder reconocer palabras clave incluso si la persona accedía a Internet por estos servidores. Estas palabras se reconocían como «contenido sensible» y se aplicaba el Protocolo de Control de Transmisiones (TCP). Para evitar este tipo de control, los usuarios (sobre todo las empresas multinacionales) comenzaron a utilizar redes privadas virtuales (VPN) para encriptar sus comunicaciones internas.
- En una tercera fase con apoyo del gobierno, los programadores del Gran Cortafuegos consiguieron reconocer y vulnerar las VPN para reducir velocidades o reiniciar las conexiones privadas. Los programadores de software libre de GitHub,

crearon una tecnología de elusión llamada Shadowsocks que encripta las comunicaciones entre el usuario y la web, a través de distintos métodos de encriptado y puertos aleatorios.

El 1 de junio de 2017 se promulgó la «Ley de Ciberseguridad» con el fin de promover la soberanía en Internet. Este marco amplía los derechos del departamento de supervisión, aumenta las responsabilidades y deberes de los operadores de Internet y exige un registro de nombres reales de usuarios. La legislación obligó a Apple a eliminar desde julio de ese año las aplicaciones VPN de su tienda de aplicaciones en China. El socio de Amazon en el país, advirtió a sus clientes que quedaba prohibido el uso de su nube para establecer un servidor VPN, ya que si las autoridades descubrían que sus clientes utilizaban VPN no aprobados, podrían cerrar sus servicios.

La presión a la que están sometidos los programadores y usuarios de VPN es severa. Desde julio del año 2019 aparecen regularmente noticias de acoso a desarrolladores y usuarios de software de proxy. Alrededor de la Gran Muralla Digital se da un enfrentamiento entre las tecnologías de "construcción de muros" y tecnologías “demoledoras de muros".

Actualmente, los internautas chinos que desean conectarse con la red externa deben elegir entre renunciar a su privacidad y suscribirse a un VPN autorizado, o vencer su temor al acoso policial y utilizar herramientas de elusión extranjeras.

En Noviembre de 2016, el gobierno chino sancionó una nueva ley de protección de datos personales para afianzar su potestad de control sobre los datos en Internet en pos de combatir el ciberterrorismo y la piratería. A partir de la regulación, las empresas que brindan servicios online no pueden recopilar y vender información personal de los usuarios y los usuarios tienen derecho a eliminar sus datos personales en casos de abuso.

El sector empresarial sintió que esta nueva regulación iba a afectar su actividad eintentaron hacer lobby para que la ley se demorara. Denunciaron que la intención era que el Estado chino reemplazara a las empresas para monopolizar toda la información.

Desde el 1 de diciembre del 2019, a partir de una regulación definida por el Ministerio de Industria y Tecnología, los proveedores de telecomunicaciones deben escanear los rostros de los nuevos clientes de servicios móviles y de datos para verificar que coincidan con sus identificaciones.[23]

Tu cara (no) me suena

Frente a este sistema de vigilancia masiva, se opone la ciudad de San Francisco, que prohibió el sistema de reconocimiento facial. Se convirtió en la primera ciudad en Estados Unidos en frenar esta tecnología policial.

[23] https://www.bbc.com/mundo/noticias-50622301

La ordenanza del ayuntamiento considera que el uso de esta tecnología potencia la represión del Estado. “San Francisco declaró que la tecnología de vigilancia es incompatible con una democracia saludable y que las personas merecen una voz en las decisiones sobre la vigilancia de alta tecnología", dijo el activista de la Unión Estadounidense por las Libertades Civiles (ACLU) Matt Cagle en el Financial Times. Uno de los concejales promotores de la medida, Aaron Peskin, utilizó como fundamento un estudio de ACLU en julio del 2018. Se puso a prueba el sistema de reconocimiento facial desarrollado por Amazon, Amazon Rekognitiion, y escanearon las caras de los 535 miembros del congreso de Estados Unidos. Se confrontaron con 25 mil imágenes públicas de sospechosos buscados por la policía. Como resultado, el sistema confundió a 28 congresistas con delincuentes y dejó expuesto el riesgo que puede suponer la aplicación de esta tecnología en la sociedad civil.

Reconocimiento Facial en Argentina

En marzo del 2011, se creó en Argentina el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) bajo el Decreto 1766/11. Se trata de un sistema de reconocimiento automatizado de huellas dactilares y rostros[24], tomadas por el Registro Nacional de las Personas (RENAPER) cuando se tramita el pasaporte o el DNI y en ciudadanos extranjeros al ingresar al país. Si las fuerzas de seguridad cuentan con una huella dactilar, la contrastan con una base de datos en la que no solo hay información sobre sospechosos, sino de todos los habitantes de la Argentina.

Los sistemas de reconocimiento facial capturan una imagen bidimensional o tridimensional de la cara de una persona y la comparan con una base de datos. Se buscan patrones sobre la geometría particular de un rostro humano: tamaño de ojos, su ubicación exacta respecto de la nariz, el grosor de las cejas, cuán prominentes son los pómulos, la medida de la frente.

Con esos datos, el sistema identifica, ante dos imágenes, si se trata de la misma persona. Esta estimación siempre tiene un margen de error. De acuerdo a la sofisticación del sistema reconoce que alguien que mira de costado es la misma persona que mira de frente, o si cambia el corte de pelo.

El Gobierno de la Ciudad de Buenos Aires incorporó esta tecnología en abril del año 2019. Se compone de 300 cámaras de video vigilancia, instaladas en las calles y subterráneos de la Ciudad, que abastecen de imágenes en tiempo real al sistema. Cuando las cámaras detectan un posible sospechoso, se notifica a las fuerzas policiales más cercanas para detener al individuo.

[24] Decreto del PEN N° 1766/11.

El software fue desarrollado por una empresa rusa y tiene una efectividad del 93%. Su acierto depende de dos elementos fundamentales: del aprendizaje, dado que cuantas más fotos analice, más preciso y eficaz será el reconocimiento y de la calidad de las imágenes, ya que será más difícil identificar patrones con poca luz o si el rostro está lejos de la cámara.

Esta herramienta forma parte del Sistema Público Integral de Video-Vigilancia y permite identificar, en menos de medio segundo, los rostros de prófugos registrados en la base de datos del Co.Na.R.C. (Consulta Nacional de Rebeldías y Capturas).

El Co.Na.R.C es una base de datos pública dependiente del Ministerio de Justicia y Derechos Humanos de la Nación. En esta base, la Justicia Federal, Nacional, las provincias y la Ciudad cargan los pedidos de captura. Cecilia Amigo, jefa de gabinete de la Secretaría de Administración, dependiente del Ministerio de Seguridad y Justicia de la Ciudad de Buenos Aires, explica que "el software únicamente detecta a aquellas personas que están en el registro de la base de datos de prófugos (…) que tienen orden de restricción impartida por la Justicia".[25] El único dato que se almacena es el de alerta positiva. Si esa persona buscada pasa por delante de la cámara, salta el alerta pero no hay tratamiento posterior de los datos de los que no están siendo buscados. Sin embargo, siempre se plantea el porcentaje en términos de margen de error que más alla de un número, en la vida real significa arrestos y detenciones a personas inocentes. Para ejemplificar la situación, en agosto de 2019, Guillermo Ibarrola fue detenido en la estación Retiro y trasladado a un penal de Bahía Blanca por 6 días ya que el sistema relacionó erróneamente su rostro con un caso de robo agravado del año 2016.[26]

Debates a nivel nacional

Estos mecanismos de vigilancia generaron una crítica tensión crítica con los derechos de Privacidad e Intimidad. La ADC (Asociación por Derechos Civiles) sostiene que “la identidad de la biometría es bifronte: una (supuestamente) positiva que nos promete traer eficiencia y seguridad a nuestras vidas y actividades; y otra negativa, que amenaza con dejar un espacio muy acotado a nuestra privacidad.[27]

“No puede haber tensión entre seguridad y privacidad", advierte Beatriz Busaniche, integrante de la Fundación Vía Libre. Un sistema que analiza todos los rostros, representa una "pérdida de seguridad, lo que implica una mayor vulnerabilidad por parte de todos". Leandro Ucciferri, analista de políticas públicas de la ADC, señala que “para que funcione tiene que identificar a todos los que pasaron. Por lo cual ya se afectan derechos de millones

[25] https://www.lanacion.com.ar/tecnologia/el-debate-detras-del-uso-camaras-seguridad-nid2243734
[26] https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

[27] https://adc.org.ar/informes/desafios-la-biometria-la-proteccion-los-datos-personales/

de personas en pos de encontrar a 40.000. (..) En este caso, se trata a todas las personas como posibles culpables." [28]

La ADC entiende que la Privacidad se alteró con el tiempo. Con el avance de lo digital, las tecnologías de la información se insertaron en la vida privada de las personas. El derecho a la privacidad está consagrado en el artículo 19[29] de la Constitución de la Nación Argentina: "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados".

Los datos biométricos obtenidos de las cámaras de seguridad deberían ser considerados como datos sensibles porque las características físicas captadas por ellas podrían revelar origen racial y étnico. Si se identifican de manera unívoca los rostros de las personas que participan de una movilización, podrían revelar opiniones políticas y convicciones religiosas. Deberían estar contemplados como una categoría de datos que debe almacenarse con recaudos especiales y utilizarse sólo en excepciones.

Reflexiones

Los estados a lo largo de la historia se han valido de las tecnologías para vigilar a la población. La novedad de los sistemas de control es el nivel de precisión y penetración en la vida de los ciudadanos, al permearse en el uso masificado de dispositivos y aplicaciones.

El nuevo paradigma de la vigilancia permite registrar aspiraciones, metas, intereses, preferencias, sentidos, rutinas de las personas para almacenarlas, jerarquizarlas y utilizarlas. Se accede a la intimidad de los ciudadanos para conocer sus patrones de acción y poder anticiparse, siempre que sea posible, a los riesgos que pueda generar. Hay acción previa del Estado sobre las libertades individuales de las personas.

¿Los ciudadanos están al tanto de que son observados sistemáticamente por panóptico omnipresente? Un sistema de vigilancia que se vale de infraestructuras en el espacio público y de aplicaciones en los propios dispositivos de los usuarios ¿Qué medidas técnicas se aplican para el cuidado de esos datos?, ¿en caso de una intromisión, se notifica a los ciudadanos de que su información pudo haber sido vulnerada? Se necesita generar un diálogo con la ciudadanía para explicitar qué se registra de ellas, con qué finalidades, por cuánto tiempo. En caso de ofrecer/obligar la descarga de aplicaciones, deben existir fuentes de código abierto y descripción de los protocolos de seguridad a disposición de los usuarios para hacer más transparente e inteligible la relación Estado-Ciudadanía.

En capítulos anteriores, se ha definido que los datos deben ser revisados ya que nada garantiza la total confiabilidad sobre los mismos. ¿Qué pasa cuando estos datos se ponen

[28] https://www.lanacion.com.ar/tecnologia/el-debate-detras-del-uso-camaras-seguridad-nid2243734
[29] http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

en juego en el Sistema de Crédito Social Chino (SCS)? Si hay un error en algún dato o no es verdadero, y se genera un falso positivo, puede haber una consecuencia concreta en el mundo real para el ciudadano. Una persona puede ser incluida en listas negras o bajar su puntaje de forma tal que se le prohíbe acceder a un tratamiento de salud en una determinada institución. ¿Cuánto tarda en hacerse efectiva una rectificación en este sistema?, ¿existen instancias claras para que los ciudadanos puedan hacer esa rectificación?, ¿qué pasa si alguno o varios ciudadanos realizan una denuncia falsa intencionalmente o no acertada sobre otra persona?, ¿cuál puede ser la consecuencia de aplicar una restricción por una conducta que luego resultó ser errónea? Existen grises que deben tenerse en cuenta a la hora de contemplar las lógicas de funcionamiento de una sociedad, con sus intencionalidades, sus pasiones, defectos, aciertos y ambiciones.

Ya en el año 1998, Lawrence Lessig en su conferencia “Las leyes sobre el ciberespacio” mostraba su preocupación por las regulaciones que el gobierno de los Estados Unidos imponía sobre las arquitecturas del ciberespacio, en materia de encriptación de contenidos para identificar y regular indirectamente (p.177). El Estado puede decidir sobre los cursos que toma este soberano a través de regulaciones e imposiciones a la arquitectura. Influye sobre cómo ese código conduce los comportamientos de la sociedad inmersa en el ciberespacio. “Debemos desarrollar en contra de este soberano los mismos límites que nosotros hemos desarrollado sobre el mundo real” (p. 179). Este soberano esconde a través de complejos códigos las fuerzas y lógicas del poder, y los intereses políticos y económicos que rigen la sociedad.

El reconocimiento facial lleva el entrecruzamiento de datos a su máxima expresión ya que ni siquiera es necesario que una persona ingrese datos en una plataforma: basta con caminar por un espacio público. Los gobiernos pueden llevar adelante un rastreo sutil y eficaz para así imponer barreras, dificultades, restricciones de derechos casi de manera automática sobre el ciudadano. Un ciudadano cada vez más acorralado por nuevos sistemas de vigilancia que desafían incluso sus posibilidades de rebelarse ante estas prácticas impuestas.

Capítulo 4: La ley divina

Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos 2016/679 conforma la legislación más completa en materia de protección de datos personales. Comenzó a aplicarse en la Unión Europea a partir del 25 de Mayo del 2018.

Este conjunto de disposiciones es de alcance extraterritorial ya que se aplica a todas las empresas (dentro y fuera de la Unión Europea) que traten datos personales de residentes de la UE para la oferta de bienes o servicios.

El Reglamento derogó la ley orgánica de protección de datos, la Directiva 95/46/CE, que reguló a la UE por más de veinte años. Unifica los criterios en materia de legislación de datos personales de todos los países de la Unión. Hasta su sanción, al tratarse de una directiva, venía acompañada de una legislación propia de cada país.

El objetivo de la normativa es dotar a los usuarios de herramientas que le permitan tener mayor control, conocimiento y propiedad de los datos de su actividad en redes sociales y servicios en línea. Se introducen disposiciones más estrictas en cuanto a la gestión de los datos personales por parte de las empresas, instituciones y organismos que deben adaptarse a estas nuevas medidas de forma proactiva, es decir, deben ser capaces de demostrar el cumplimiento.

Desde el diseño y por defecto

El Reglamento obliga que los responsables de tratamiento cumplan con la protección de los datos “desde el diseño y por defecto”.

Desde el diseño significa que el responsable deberá tener en cuenta las medidas de seguridad desde el momento en el que define los sistemas de almacenamiento de los datos. Debe aplicar recursos técnicos como la seudonimización. Este proceso consiste en sustituir un atributo único por otro en un registro para reducir la posibilidad de vincular un conjunto de datos con la identidad del interesado. Esa vinculación, igualmente, no puede ser eliminada del todo, por lo que siempre habrá probabilidad de identificar a la persona física de manera indirecta si se consigue recuperar el atributo inicial. Un ejemplo sería sustituir el nombre de un usuario por un número de identificación (más conocida como ID).

El cumplimiento de la normativa por defecto obliga a la empresa a adoptar la configuración de privacidad que más resguarde los datos de sus clientes y evite las brechas de seguridad.

La protección de datos personales en los contextos digitales

En el primer apartado del Artículo 4, la normativa define a los datos personales como

> “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”.

En el considerando inicial 51, se prohíbe el tratamiento de una categoría de datos especiales “que por su naturaleza son particularmente sensibles en relación con los derechos y las libertades individuales ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales”. Se incluyen en este grupo datos personales que revelen el origen étnico o racial, opiniones políticas, “convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física”.

La Unión Europea ya había consagrado el derecho que toda persona tiene “a la protección de los datos de carácter personal que la conciernan” en el Artículo 16 del Tratado de Funcionamiento de la Unión Europea del año 1957 y también en el Artículo 8 de su Carta de Derechos Fundamentales proclamada el 7 de Diciembre del año 2000: “estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada (...) Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y su rectificación”.

En el considerando inicial 2, se establece que:

> “los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular, el derecho a la protección de los datos de carácter personal”.

Se define que “el tratamiento de los datos personales debe estar concebido para servir a la humanidad”.

En el segundo apartado del Artículo 4, concibe al tratamiento como:

> “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o

> modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

En el considerando inicial 6, el Reglamento atiende a la urgencia de actuar sobre los cambios en los contextos de trabajo y funcionamiento de las sociedades. Platea la necesidad de revisar el marco legal para no vulnerar la privacidad de los ciudadanos:

> "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales."

Cualquier tipo de tratamiento de datos debe estar legitimado sobre una base que justifique la solicitud y almacenamiento de información. El Reglamento enumera las siguientes legitimaciones:

- Obligación Contractual.
- Obligación Legal para el responsable (por ejemplo, se piden datos por requerimientos fiscales, para la confección de facturas se necesita cierta información del cliente).
- Intereses vitales del interesado o de otras personas.
- Misión de Interés Público o ejercicio de poderes públicos.
- Si el recabado de datos no se encuentra encuadrado en estas categorías, las empresas o dependencias públicas tienen la obligación de solicitar un consentimiento.

El nuevo consentimiento

El Reglamento obliga a las empresas e instituciones públicas a solicitar un consentimiento explícito al usuario. Debe ser correctamente registrado para probar su existencia en caso de que la autoridad de aplicación lo solicite.

En el considerando inicial 32, se aclara que el consentimiento debe "darse mediante un acto afirmativo claro que refleje la manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le

conciernen". Antes del Reglamento, el consentimiento era tácito o por omisión, es decir, se basaba en la inacción (por ejemplo "al utilizar nuestros servicios usted también autoriza que sus datos puedan ser utilizados para remitir información comercial"). El consentimiento debe habilitarse mediante un formulario en papel o web que incluya una casilla en la que se aceptan términos, condiciones y política de privacidad. Esta casilla debe estar desmarcada por defecto para que el usuario tenga que realizar la acción explícita de seleccionar el casillero. Quedan terminantemente prohibidas las casillas ya marcadas de manera predeterminada. Esta instancia debe estar presente antes de que se puedan empezar a recabar los datos y, en caso de que los usuarios ya tuvieran actividad en una plataforma, se debe actualizar el consentimiento (por ejemplo, solicitar nuevamente la autorización para el envío de publicidad).

La solicitud de consentimiento debe expresarse en un lenguaje claro, conciso y sencillo para garantizar que el usuario comprende al menos los puntos salientes de aquello que acepta (aunque en la profundidad de las condiciones, es difícil que el usuario promedio alcance a entender la totalidad de lo que habilita a hacer con sus datos). El principio fundamental del reglamento es el de Transparencia que "exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender" (considerando inicial 39). El consentimiento debe darse para todas las actividades de tratamiento que se harán sobre esos datos: "los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos(...) Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados". Cuando el tratamiento tenga varios fines, el usuario debe autorizar los usos adicionales y se le debe ofrecer la posibilidad de retirar el permiso cuando lo considere.

El consentimiento deberá ser explícito en caso de transferencias internacionales (si la información será tratada por empresas de países fuera de la Unión Europea). También en los casos en los que se aplican decisiones automatizadas sobre los datos.

Lo que se busca es el tratamiento leal y transparente para minimizar patrones de discriminación y exclusión (atendiendo al derecho a la no discriminación): "El interesado debe tener derecho a no ser objeto de una decisión (...) que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar" (considerando 71).

El usuario debe ser informado si sus datos personales serán utilizados para la elaboración de perfiles, procedimiento que el Reglamento en su Artículo 2 (punto 4) define como:

> "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud,

preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

El usuario podrá solicitar que las decisiones automatizadas sean revisadas por personas, y estará habilitado para "expresar su punto de vista y a impugnar dicha decisión". También podrá pedir al responsable de tratamiento especificaciones del funcionamiento del algoritmo que actúa en esas operaciones.[30]

El Reglamento exige que el consentimiento incluya de manera clara:

- Identidad del responsable del tratamiento de los datos que el usuario cederá.
- La legitimación que autoriza que ese responsable almacene y recoja los datos (si los datos se solicitan porque media un contrario, una obligación legal o hay un consentimiento del usuario en la que se apoye).
- Los destinatarios de esos derechos.
- La fuente de procedencia en caso de que los datos se hayan obtenido de un tercero.
- Hacer referencia a los derechos que tiene el usuario sobre sus datos.

Nuevos derechos

El Reglamento amplía y refuerza los derechos de los usuarios. En cuanto a los derechos ya existentes, se reconocen:

- **Derecho de Acceso**: los usuarios tienen derecho a saber qué datos maneja una empresa sobre su persona y qué tipo de tratamiento hace.
- **Derecho a Rectificación**: el usuario puede solicitar que sus datos sean revisados, actualizados y corregidos en caso de que los mismos sean inexactos o incompletos (si los datos personales compartidos son incorrectos, puede ser necesario también informar a todos los que los hayan consultado).
- **Derecho a Supresión**: los usuarios pueden solicitar que se eliminen sus datos cuando ya no son necesarios para el cumplimiento del objetivo inicial por el que se solicitaron, si retira su consentimiento o si se han vencido los plazos y no existe otra base legal para el tratamiento.
- **Derecho a Oposición**: los usuarios pueden oponerse al tratamiento de sus datos personales cuando no sea requerido el consentimiento, se utilicen con fines publicitarios o se traten para tomar una decisión referida al titular.

Los nuevos derechos que crea el nuevo Reglamento son:

[30] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_es

- **Derecho a la Portabilidad**: las personas pueden solicitar los datos personales que haya facilitado a un responsable de tratamiento para transferirlos a otro. La información debe ser entregada en formato legible, de lectura automática mecánica, de uso común e interoperable para que pueda ser incorporada fácilmente a otro sistema.
- **Derecho al olvido**: el usuario le puede solicitar a la empresa que, además de suprimir los datos de sus bases, debe inhabilitarlos de sus entornos y publicaciones digitales: dar de baja todas las indexaciones que vinculan su nombre con un contenido (por ejemplo, los links). El responsable del tratamiento está obligado a exigir a terceros que trabajan con esos datos que supriman todo enlace a ellos, sus copias o réplicas.

Delegado de Protección, Autoridad de Aplicación y Sanciones

El Reglamento crea la figura del Delegado de Protección de Datos: responsable de supervisar cómo se tratan los datos personales para velar por el cumplimiento de la normativa. El delegado coopera con la autoridad de protección de datos y media en la relación entre las autoridades y los ciudadanos. La persona designada debe estar formada en el ámbito del derecho y debe actuar de manera independiente. Esta figura es obligatoria para organismos públicos, empresas que manejan datos a gran escala, colegios profesionales, empresas del sector médico, centros docentes, entidades aseguradoras, publicidad y prospección comercial.

En caso de que se produzca una brecha de seguridad por la que se haya vulnerado la confidencialidad de los datos, las empresas deben informarlo a la Agencia de protección dentro de las 72 horas posteriores al hecho.

Las sanciones que se aplican por el incumplimiento del Reglamento pueden alcanzar los 20 millones de euros o, en infracciones más graves, multas que representan el 4% del volumen del valor de los negocios mundiales totales de la empresa. Además, se puede inhabilitar a las empresas a seguir tratando bases de datos.

La Autoridad de Aplicación del Reglamento es definida por cada uno de los estados de la UE. Se trata de Autoridades de Protección de datos públicas e independientes, encargadas de supervisar la aplicación de la legislación y aplicar sanciones.[31]

El Reglamento en la práctica

[31] En este link se pueden consultar las autoridades de aplicación de cada país miembro de la Unión Europea https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

Al momento de realizar la tesina, el Reglamento ya contaba con dos años de vigencia, por lo que es posible analizar el nivel de cumplimiento y las sanciones que aplicaron las autoridades.

En un informe de octubre del 2019, el Instituto de Investigación Capgemini[32], centrado en el impacto de las nuevas tecnologías en las empresas, reveló que sólo el 28% de las organizaciones y empresas habían cumplido con la implementación completa del Reglamento, mientras que el 30% estaban en camino de alcanzarla. La encuesta se realizó a 1.100 ejecutivos de sectores bancarios, venta de productos de consumo, servicios públicos, telecomunicaciones y atención médica. Las mayores dificultades con las que se enfrentaron a la hora de implementar el reglamento incluyen "la complejidad de los requisitos del Reglamento (36%), los costes de su implementación (33%) y los desafíos que plantean sus infraestructuras tecnológicas heredadas (38%)"[33].

Los países que más se adaptaron al Reglamento fueron Estados Unidos (35%), seguido de Reino Unido y Alemania (en ambos, un 33%). España e Italia (en ambos países, un 21%) y Suecia (18%) se ubicaron entre los últimos puestos

La inversión estimada para adaptarse al Reglamento alcanzaba más del millón de dólares, al contemplar honorarios legales a profesionales y actualizaciones tecnológicas.

Durante el primer año de aplicación del Reglamento, se incrementaron las solicitudes de información a tal punto que el 50% de las empresas estadounidenses recibieron 1000 solicitudes de información.

El 1º de Julio de 2020, el portal español elEconomista publicó un artículo periodístico[34] en el que hace un balance de los criterios de aplicación y ejecución del Reglamento. Uno de los principales objetivos de la nueva normativa es la unificación del marco jurídico en materia de protección de datos personales. Sin embargo, son llamativas las diferencias en cantidad y monto de las multas que se aplicaron en cada país. En España, la Autoridad de Aplicación (Agencia de Protección de Datos) llegó a imponer 112 multas en el 2019 (un 70% menos que el año anterior). Las sanciones alcanzaron un valor total de 6.3 millones de euros, repartidas en "directorios (2.9 millones de euros), telecomunicaciones (641.000), contrataciones fraudulentas (620.620) y quiebras de seguridad (460.000)". Garante, la autoridad de control de Italia, impuso 10 multas que sumaron un total de 40 millones de euros. En Alemania, se expidieron 13 multas que alcanzaron los 25 millones de euros. En el Reino Unido, ICO (Information Commissioner's Office) sancionó a British Airways por 204 millones de euros, luego de identificar que la empresa no cumplía con las medidas básicas

[32] https://www.capgemini.com/mx-es/wp-content/uploads/sites/24/2019/09/Las-empresas-se-han-rezagado-en-el-cumplimiento-de-GDPR.pdf

[33] https://www.eleconomista.es/economia/noticias/10109134/09/19/Las-grandes-empresas-espanolas-entre-las-mas-atrasadas-en-proteccion-de-datos.html

[34] https://www.eleconomista.es/opinion-blogs/noticias/10639960/07/20/RGPD-balance-de-dos-anos-y-una-aplicacion-no-tan-armonizada-en-la-UE.html

de seguridad para las transacciones con tarjetas, ni tenía encriptado sus códigos de seguridad[35]. Otra sanción destacada fue la de 110 millones a Marriott Hotels, por una brecha de seguridad. En Francia y en Polonia, se han impuesto, desde el 25 de mayo de 2019, solo seis multas que ascienden a 1,3 millones de euros y cinco multas por un total de 710.000 euros, respectivamente. En enero del 2019, Francia sancionó a Google por 50 millones de euros al reconocer "falta de transparencia, información incorrecta y ausencia de consentimiento válido en la publicidad personalizada"[36]. La Comisión Nacional de Informática y Libertades, acusó a la empresa de violar los principios de transparencia, información y consentimiento, y de dejar "a los usuarios sin sus garantías esenciales ya que practica operaciones que pueden revelar importantes partes de la vida privada" en el tratamiento de la información para la personalización de los anuncios.

Ley de Protección de Datos Personales en Argentina

En octubre del año 2000, se sancionó la ley Nº 25.326 sobre Protección de los Datos Personales. Fue reglamentada por el Decreto 1558/01 y se basó en la ley española de 1992.

Definiciones generales

La ley 25.326[37] define en su Artículo 1º que el objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean públicos o privados destinados a dar informes.
Se basa en dos garantías de la Constitución Nacional:

- Artículo 19: Derecho a la intimidad y honor.

> "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

- Artículo 43 (tercer párrafo) incorporado en la reforma de 1994. HÁBEAS DATA

> "toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o

[35] https://cincodias.elpais.com/cincodias/2019/07/29/legal/1564410687_469515.html

[36] https://www.abc.es/tecnologia/redes/abci-francia-multa-google-50-millones-euros-falta-transparencia-201901211634_noticia.html#vca=mod-sugeridos-p1&vmc=relacionados&vso=francia-multa-a-google-con-50-millones-de-euros-por-falta-de-transparencia&vli=noticia.foto.tecnologia

[37] http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

> discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos".

Se trata de una garantía que el Estado otorga a los ciudadanos para proteger el derecho de protección de datos personales. Se entiende como garantía a una "herramienta que permite remover un obstáculo que impide el goce de un derecho reconocido o reponerlo en caso de que haya sido violado". (Guida, Himelfarb, Sanchez Porto, 2009, p.4).

La ley en su Artículo 2 define a los datos personales como "la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". Al igual que en el RGPD, distingue la categoría de datos sensibles:

> "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

Ninguna persona debe ser obligada a proporcionar ninguno de estos datos (Artículo 7). El Reglamento define e incluye en esta categoría a los datos genéticos y datos biométricos[38].

La ley argentina obliga a los responsables de las bases de datos a registrarse en el órgano de control.

En el artículo 5, se exige el consentimiento del titular para que el tratamiento de los datos sea lícito. El consentimiento debe ser "libre, expreso e informado" y "deberá figurar en forma expresa y destacada" antes de recabar la información. De lo contrario, el tratamiento será ilegal a menos que:

- Se obtengan de fuentes de acceso público irrestricto.
- Se recaben para el ejercicio público de funciones propias de los poderes del Estado o por obligación legal.
- Bases que incluyen sólo nombre, DNI, identificación tributaria o previsional, fecha de nacimiento, domicilio.
- Datos que deriven de una relación contractual, científica o profesional del titular de los datos.
- Se trate de operaciones de entidades financieras con datos que reciban de sus clientes.

El artículo 9 de la ley obliga al responsable o usuario del archivo de datos a adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad

[38] El RGDP define en el artículo 4 a los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

de los datos personales. Se busca evitar su adulteración, pérdida, consulta o tratamiento no autorizado producidas por desviaciones, intencionales o no, de información.
El deber de confidencialidad está contemplado en el artículo 10: el responsable y las personas que intervengan en cualquier fase del tratamiento de datos están obligados al secreto profesional.
La ley 25.326 prohíbe las transferencias internacionales de datos personales a países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

Derechos de los titulares y autoridad de aplicación

En lo que respecta al derecho de información, la ley garantiza en su Artículo 43 que toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de esos responsables. La consulta es pública y gratuita, y se realiza a través del Registro Nacional de Bases de Datos (creado por el organismo de control -Dirección Nacional de Protección de Datos Personales- en el año 2005).
En referencia al derecho de acceso, la ley sostiene en el Artículo 14 que el titular de los datos tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a dar informes. El responsable o usuario cuenta con 10 días corridos para responder la solicitud de forma clara, sin codificaciones técnicas y acompañada de una explicación en lenguaje accesible en caso de que la información sea muy compleja.
En el Artículo 16, se les concede a los usuarios los derechos de rectificación, actualización o supresión de los datos personales de los que sea titular en un banco de datos. Se busca garantizar el principio de calidad de los datos que establece que “deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido (...) no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención”. El responsable o usuario del banco de datos debe dar curso a la solicitud en un plazo máximo de cinco días hábiles de recibido el reclamo.
Originalmente, la ley definió a la Dirección Nacional de Protección de Datos Personales (DNPDP) como autoridad de control, un órgano con autonomía funcional y descentralizada en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Con la reforma de la Ley de Ministerios 746/2017, se modifican las atribuciones de la Agencia de Acceso de la Información Pública (AAIP) y se le agrega la función de autoridad de protección de datos. La DNPDP fue absorbida por la AAIP que tiene carácter autárquico y posee autonomía funcional dentro del ámbito del Poder Ejecutivo.

Sanciones y caso práctico

En el Capítulo VI, se definen las sanciones que contemplan desde apercibimientos y suspensiones, hasta la imposición de multas (de $1000 a $100.000) y la cancelación de las bases de datos. La gran diferencia con el RGDP, es el valor máximo que pueden alcanzar las sanciones económicas a los responsables del tratamiento de datos. El monto que pueden alcanzar las multas en la UE es mucho mayor que en Argentina. Esto se debe a que el Reglamento toma en cuenta el porcentaje del negocio total de la empresa para definir los valores de las multas, mientras que en Argentina los montos son fijos, en pesos, muy bajos y desactualizados respecto de los recursos de las empresas que concentran la actividad del tratamiento de los datos.

En mayo del 2020, la Agencia de Acceso a la Información Pública impuso a Google Argentina SRL y Google LLC una multa de 280.000 pesos por incumplir con la ley de datos personales[39]. En septiembre del 2019, un tercero no autorizado ingresó en la cuenta de Gmail de Micaela Giolito, modificó su contraseña y eliminó el historial de acceso de todos los dispositivos que estaban vinculados a su cuenta. Micaela perdió el acceso a toda la información en las diferentes aplicaciones de Google (carpetas de Drive, preferencias de Youtube, recorridos de Google Maps).

La afectada envió una carta documento a la sede de Google Argentina SRL para solicitar la restitución de su información. La empresa respondió que no era la encargada del manejo de los servicios de Gmail y la derivaron a la casa matriz, Google LLC, en California (Estados Unidos). Luego de intentar comunicarse sin éxito, Micaela recurrió a la Agencia e inició una medida judicial. El organismo concluyó que, que con su accionar, Google Argentina SRL y Google LLC incumplieron con la Ley 25.326 de Protección de Datos Personales.

Luego del fallo[40], el exdirector de la Agencia de Acceso a la Información Pública, Eduardo Bertoni, declaró que “en comparación con las sanciones que se imponen en Europa, en nuestro país las sanciones previstas por la ley son económicamente bajas. En consecuencia, actualizar nuestra Ley de Protección de Datos Personales es una necesidad cada vez más evidente”.[41]

Bertoni, desde el año 2016, es uno de los principales impulsores del debate de una nueva ley de datos personales. Para delinear una nueva legislación en la materia, se convocaron actores del sector privado, la sociedad civil y el ámbito académico que contribuyeran a conformar una visión acabada del camino a seguir y de las particularidades nacionales a tener en cuenta.

[39] https://www.telam.com.ar/notas/202005/465522-multan-en-la-argentina-a-google-por-no-permitir-a-una-usuaria-acceder-a-sus-datos-personales.html
[40] Fallo original: https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf
[41] https://www.argentina.gob.ar/noticias/sancion-google-por-negar-el-derecho-de-acceso

El resultado fue un proyecto de ley que incluyó muchos de los conceptos introducidos por el RGPD, entre los cuales se destacan:

- ¶ Se incluyen y definen los datos biométricos y datos genéticos dentro de la categoría de datos personales.
- ¶ Se obliga a los responsables de tratamiento de notificar a la autoridad de aplicación en caso de que se produzcan brechas de seguridad en sus bases.
- ¶ Se introduce la figura del Delegado de Protección de datos que es obligatorio para organismos públicos y empresas que traten datos sensibles y a gran escala.
- ¶ Se actualizan los montos de las sanciones económicas, que pueden llegar a ser equivalentes al valor de quinientos salarios mínimos vitales móviles al momento de la violación de la ley.
- ¶ Se crean nuevos derechos: el derecho a la portabilidad de los datos personales y el de oposición de los usuarios en caso de ser objeto de decisiones automatizadas.

Este proyecto de ley finalmente perdió estado parlamentario. Mientras tanto, los datos de los usuarios siguen siendo regulados por una ley sancionada hace dos décadas.

La escritora y periodista Marta Peirano argumenta que, al abrir una cuenta en alguna plataforma, se genera una relación íntima entre el usuario y el servidor, lo que llama "engagement": "porque entre las dos partes se interpone un contrato prenupcial que el usuario debe aceptar como una novia agradecida, sin modificaciones ni anexos, llamado Términos de uso." (2018, p.19). En el año 2015, los términos de iTunes contenían veinte mil palabras y los de Facebook quince mil, divididos en múltiples segmentos y con un complejo lenguaje, difícil de entender por un usuario promedio.

"Las Constituciones, los códigos y las leyes han sido dictados para el universo material, para la presencialidad, para los espacios físicos delimitados por fronteras, para mercaderías tangibles que pasan por aduanas, para monedas reales" (Aguiar, 2007, p.173). Es necesario plantear una legislación que pueda hacer frente a las nuevas amenazas a la privacidad que pueden generar las nuevas tecnologías.

Los titulares de los datos deben contar con instancias de información claras para que comprendan qué información ceden y bajo qué términos. Deben estar protegidos frente a filtraciones o brechas de seguridad que vulneren la privacidad e intimidad.

Deben replantearse las sanciones y los montos de las multas para que se mantengan actualizadas. De lo contrario, si los valores son bajos, los riesgos y consecuencias que acarrean para las grandes empresas no significan una amenaza ya que cuentan con los recursos para pagarlas.

Reflexiones

La identidad analógica y la digital están cada vez más relacionadas. Lo primero que se suele hacer cuando se quiere indagar sobre la vida de una persona es buscarla en internet. En cuestión de segundos, se pueden explorar sus perfiles de Instagram, Facebook, Linkedin, su blog personal, las firmas que pudo haber hecho para algún petitorio, los retweets que realizó de ciertas figuras públicas. Infinidad de links que relacionan un nombre con contenidos.

Hablar de perfiles digitales es alejarse cada vez más de la privacidad. Pero, ¿qué es la privacidad? Es aquello sobre lo que se tiene control para proteger de cualquier intromisión. Con los avances tecnológicos y la diversificación de técnicas de tratamiento de datos, la vida privada paso de "ser concebida en términos de la libertad negativa de rechazar u oponerse al uso de la información personal para transformarse en la libertad positiva de supervisar su uso" (Guida, Himelfarb, Sanchez Porto, 2009, p.4). "Igual que la imprenta preparó el terreno para las leyes que garantizaban la libertad de expresión –que no existían antes, al haber tan poca expresión escrita que proteger–, la era de los datos masivos precisará de nuevas reglas para salvaguardar la inviolabilidad del individuo" (Cukier Mayer-Schönberge, 2013, p.15)

El derecho al olvido, introducido en el RGPD, puede significar para los usuarios un mayor margen de control sobre la disponibilidad de sus datos en internet. Sin embargo, se generan nuevas tensiones entre los derechos de protección de datos, el honor y la reputación con el derecho a la información y a la libertad de expresión. La Declaración Universal de los Derecho Humanos, en su artículo 19, como la Convención Interamericana de Derechos Humanos, en su artículo 13, definen el derecho a la opinión, a la crítica y a la pluralidad de contenidos como condiciones necesarias para la calidad democrática de la sociedad.

Se trata de conceptos y límites que en la práctica pueden ser muy difíciles de definir y hacer primar unos sobre otros. Por ejemplo, si el nombre de una persona es citado en una nota periodística como testimonio por ser partícipe de una marcha, ¿puede ser suprimido o eliminado el link que vincula su nombre con el contenido en cuestión? Más allá de que la persona no quiera ser asociada a ese evento, ¿hasta dónde se vulnera el derecho a la información del resto de los usuarios? Si un funcionario fue condenado por un delito de corrupción y cumplió su pena ¿puede solicitar que se remueva cualquier link que vincule su nombre con el hecho en cuestión? Si ya completó la sanción impuesta ¿por qué debe seguir relacionado con este delito? Sin embargo, ¿cuál es el lugar del derecho a la información de la sociedad y el interés público para el que es relevante tener memoria sobre estos hechos?

En mayo del 2019, la Agencia de Acceso a la Información Pública realizó una encuesta nacional a 4.400 ciudadanos mayores de 16 años respecto al nivel de conocimiento que se tiene sobre el derecho a la protección de datos personales[42]. La primera pregunta consistía

[42] https://www.argentina.gob.ar/noticias/cuanto-sabemos-de-datos-personales

en indagar si las personas conocían la existencia del derecho. Sólo el 33.8% de los encuestados afirmó estar informado del derecho, mientras que el 40.5% negó estar al tanto y el 25.7% restante expresó que no sabía qué responder frente a este interrogante. Aunque existan los instrumentos legales a partir de los cuales la ciudadanía puede hacer ejercer el derecho, no hay instancias informativas suficientes para que sean conocidos por la sociedad. Por ejemplo, los derechos que los titulares tienen sobre sus datos, ya sea en Argentina o en la Unión Europea, suelen figurar como un punto más dentro de una extensa lista de incisos y especificaciones legales al momento de solicitar el consentimiento.

Por lo general, son pocos los usuarios que acceden al detalle de términos y condiciones y leen detenidamente toda la información, sumado a que suele estar presentada en un lenguaje propio del campo del derecho. Entonces ¿alcanza con exigir solamente un consentimiento por parte de los usuarios para garantizar que son plenamente conscientes de lo que ceden, y del nivel de control que las empresas tienen sobre su vida virtual?

A pesar de que ese consentimiento implique una acción expresa del titular de los datos ¿no se termina convirtiendo en una sucesión de “hacer clics” en casilleros para poder tener acceso a plataformas y sitios web de manera rápida? Debería existir la obligación de exigirles a los agentes de tratamiento de información que destinen espacios para informar a los usuarios de la existencia de las herramientas con las que cuentan para tener control sobre sus datos. Por ejemplo, las aplicaciones podrían enviar notificaciones o mails para explicar que dentro de su interfaz cada usuario puede chequear su base completa de datos. Si se toma el caso de Facebook, cualquier persona puede solicitar y descargar el registro completo de su actividad en la red social. Sin embargo, no es una solicitud fácil de encontrar en la plataforma, sino que es necesario ingresar a la sección de configuración y pasar por varios menúes y submenúes hasta encontrar el botón que permite generar esa información y descargarla. Esta posibilidad de solicitud de acceso ni siquiera era conocida por la propia investigadora previo a la realización de la tesina. El público que accede a Facebook no siempre está familiarizado con la tecnología ni tampoco conoce todas sus funciones.

El consentimiento es la herramienta legal que autoriza a las empresas a trabajar con los datos de los usuarios. Sin embargo, se carga al usuario con la responsabilidad de estar al tanto de lo que acepta. No se le ofrecen instancias fácilmente accesibles que recalquen o recuerden las condiciones de uso, o los instrumentos con los que cuentan para defender su derecho de protección de datos.

Así como las plataformas o sitios web incluyen espacios de publicidad intercalados con los contenidos propios, debería existir legalmente la obligación de destinar un porcentaje de lo que se ve en la pantalla a mensajes que recuerden a los usuarios los instrumentos legales con los que cuentan en un lenguaje coloquial. Una alternativa sería un “¿sabías que podés acceder a tus datos o podés pedir la actualización de los mismos?”.

Las nuevas legislaciones obligan a las empresas/organismos a notificar a las autoridades de aplicación sobre las brechas de seguridad que puedan haberse producido en sus bases de datos. ¿Qué garantiza que efectivamente se reporten estas intrusiones? Si las sanciones que debe enfrentar una empresa pueden limitar su trabajo con bases de datos en el futuro o se trata de multas muy elevadas, ¿habrá una notificación directa de un hackeo o tratará de ocultarse?, ¿se hará explícita que la infraestructura de seguridad con la que se contaba no estaba preparada? En caso de la situación se hiciera de público conocimiento, podría generar desconfianza por parte de los usuarios que podrían optar por migrar a otras plataformas, por lo que las consecuencias para una empresa podrían ser un antes y un después para su continuidad. Por ello cabría preguntarse si las regulaciones realmente garantizan que este tipo de hechos de intrusión sean comunicadas a las autoridades pertinentes o sean aún más ocultadas por las empresas.

Se pueden generar otros nuevos escenarios de conflicto. Por ejemplo, ya fueron varios los casos Ransomware (Ransom en alusión a rescate, ware a programa). Se trata de un novedoso tipo de hackeo que encripta los archivos de una computadora al estilo de un candado virtual: “los documentos no se borraron ni se fueron; solo se transformaron de modo tal que no es posible leerlos sin esa llave aunque estuvieran ahí” (Davidovsky, 2020, p 162). La información es tomada de rehén convirtiéndola en una “sopa de bits incomprensible” (Torres, 2017, p 190). Para conseguir la llave que permita recuperar esa información, las empresas o dependencias públicas deben pagar a los hackers una determinada suma (por lo general en bitcoins porque dificulta el seguimiento virtual).

Debido a las consecuencias que puede acarrear para los responsables de las bases, ya sea por pérdida de confianza de los usuarios o por las multas que se le pueden imponer por parte de las autoridades de aplicación, generalmente se pagan estas cifras y no se hacen las denuncias pertinentes para que el hecho no trascienda en la esfera social. Algunas empresas guardan parte de sus recursos económicos en caso de que tengan que hacer frente al pago de algún tipo de extorsión o hackeo.

El problema no reside en el costo económico que puede significar para las empresas pagar estas sumas, sino el impacto que puede tener en los titulares de los datos que esa información caiga en manos de terceros. Si los datos no están lo suficientemente anonimizados, nada asegura que por más que se pague un rescate, no se haya hecho una copia externa que luego pueda ser utilizada para extorsionar a una persona incluida en las bases vulneradas. El costo social es el que se debe tener en cuenta: el riesgo al que está sometida la privacidad de los usuarios que no cuentan ni con los recursos técnicos ni económicos para defenderse.

Se necesita que existan múltiples y permanentes instancias de auditoría por parte de los organismos de control para poner a prueba las infraestructuras de seguridad de las bases registradas.

Es necesario mantener las legislaciones actualizadas a la luz de los nuevos fenómenos sociales. Debe existir participación de diversos agentes de la sociedad civil que puedan plantear las implicancias éticas, psicológicas, económicas de los contextos digitales.

La regulación en materia de bases de datos todavía no contempló la aparición de las megaplataformas y los servicios de computación en la nube. Un titular de un sistema de la nube tiene en su poder múltiples bases de datos de los usuarios que utilizan las diversas plataformas alojadas en su infraestructura. La relación directa que se establece entre las plataformas crea actores de nivel superior detrás de esas bases de datos, que pueden actuar y manejar transversalmente el conjunto de esas bases.

Se construyó un universo de distancias que tienden a esfumarce. Hasta ahora, se han definido bases de datos como entidades autónomas de las plataformas y la nube en la que se desarrollan. La concentración de plataformas multiservicio llega a consolidar pocos actores que tienen el control del sistema informático mundial. El mundo se encuentra atravesado por una nueva interacción tecnología-empresario-política cada vez más difícil de distinguir que actúa por encima de cualquier regulación. Frente a actores con tanto poder, ¿qué margen de acción le queda al usuario cada vez más inmerso en las nuevas tecnologías?

Capítulo 5º: ¿Solistas, dúos o cuartetos?

Sin políticas que aseguren la competencia, la innovación en el campo de IA tiende a conformar mercados oligopólicos o monopólicos. “Los líderes del mercado están determinados por el acceso a los datos, el poder de cómputo, los talentos altamente calificados para programar algoritmos y la propiedad de todos estos desarrollos” (Mialhe, Lannquist, 2018, 224). Los estados y las principales empresas recopilan más datos de usuarios, contratan profesionales más formados y tienen más recursos para invertir en hardware y software de procesamiento y análisis en la nube.

El mercado mundial está dominado por las empresas estadounidenses Google, Amazon, Facebook, Apple y Microsoft (GAFAM) y las asiáticas Baidu, Alibaba, Tencent y Xiaomi (BATX). La mayor parte de los desarrollos en procesamiento de datos está concentrada en estas empresas, que además tienen el poder de identificar y adquirir potenciales competidores.

A grandes rasgos, existen tres tipos de monopolio:

1. **Monopolio natural**: escenarios en los que la forma más sensata y económicamente viable de ofrecer un servicio es a través de un único prestador. Requiere control del Estado para evitar abusos de precios y garantizar la inversión en niveles previamente determinados.
2. **Monopolio de derecho**: en base a un interés general debidamente fundado, una norma define quiénes son los actores que pueden ofrecer determinados bienes y/o servicios. El Estado debe llevar adelante exhaustivas auditorías para hacer un seguimiento del cumplimiento de las metas.
3. **Monopolio de hecho**: podría haber muchos prestadores pero hay uno sólo, sin que haya una legislación que lo establezca.

En junio del 2019, el Subcomité de Derecho Antimonopolio, Comercial y Administrativo de los Estados Unidos inició una investigación sobre el estado de la competencia en línea. Este órgano tiene como misión investigar los factores que dañan la competencia y conforman monopolios, que afectan a las pequeñas empresas y los derechos de los usuarios. Analizó el dominio de Amazon, Apple, Facebook y Google, y las prácticas comerciales que aplican para reproducir su posición monopólica. El Subcomité demostró una alarmante preocupación por los niveles de concentración que alcanzaron estas plataformas: se delineó un escenario que impacta en la innovación, la calidad de los productos, la oferta a los usuarios, la democracia y la privacidad. Tal como puntualiza en la introducción de la investigación, ya a principios del 1900, el juez de la Corte Suprema, Louis Brandeis, explicó

“debemos tomar nuestra decisión. Podemos tener democracia, o podemos tener riqueza concentrada en manos de unos pocos, pero no podemos tener ambas" (p. 7).

Cada una de estas empresas se consolidó como “guardián de un canal clave de distribución” (p. 6). Esta posición dominante tiene consecuencias para los usuarios que utilizan las plataformas para interactuar, y para las empresas que las necesitan para desarrollar sus negocios.

Tradicionalmente, los monopolios conducen a la fijación de precios elevados y la reducción de la calidad de los productos y servicios. ¿Qué sucede en el mercado de plataformas que “no cobran” un precio monetario? Estos servicios se monetizan con los datos y la atención de los usuarios. Entonces el monopolio en este mercado se mide por la creciente capacidad de erosionar la privacidad de los usuarios a través de la recolección y tratamiento de más datos. En julio del 2020, la Autoridad de la Competencia del Reino Unido (CMA) también realizó una investigación sobre el mercado digital y concluyó que Google y Facebook hacen una indiscriminada recolección y uso de la información personal para la publicidad personalizada. Esto demuestra que estas plataformas no enfrentan ninguna limitación de competencia.[43]

¿Cuáles son las consecuencias para terceras empresas que deben utilizar estas plataformas para desarrollar su actividad económica? Fijación de precios predatorios, cambios en los términos y condiciones sin previo aviso, cobro de peajes o cánones por las ventas, cambios repentinos y sutiles en algoritmos que impactan directamente sobre el tráfico a una página web.

¿Cual es el problema de la formación de semejantes monopolios en la economía de las plataformas? Como tienen un rol cada vez más crítico en la interacción social, la vida académica y el consumo de productos y servicios, los usuarios están cada vez más dispuestos a resignar su información ya que no consideran viable la posibilidad de abandonar las plataformas. Esto mismo sucede para las empresas que deben aceptar condiciones abusivas ya que les resulta inevitable estar en los acotados canales por los que circulan millones de personas.

Plataformas: el nuevo modelo de negocios

Las plataformas son las protagonistas de la nueva economía. Para describirlas Nick Srnicek se aleja del análisis que las coloca como actores buscando poder y las inserta en el modo capitalista de producción: un sistema que “exige que las empresas busquen constantemente nuevos caminos para obtener ganancias, nuevos mercados, nuevos commodities y nuevos métodos de explotación” (2018, p. 13).

[43] https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

Tal como se abordó en el capítulo 1, el abaratamiento de los costos de almacenamiento, el desarrollo de técnicas de tratamiento de datos y la huella que genera la digitalización de los procesos sociales, permiten que los datos sirvan a funciones capitalistas, "educan y dan ventaja competitiva a los algoritmos; habilitan y dan coordinación y deslocalización de los trabajadores y permiten la optimización y flexibilidad de los procesos productivos" (2018, p. 44).

Las plataformas se construyen en este ecosistema como "infraestructuras digitales que permiten que dos o más grupos interactúen" (p. 45). Se trata de intermediarias que vinculan espectadores con entretenimiento, compradores con objetos físicos, trabajadores con empresas. Las considera como infraestructuras puesto que brindan a los usuarios las bases sobre las cuales sentar sus propios negocios o proyectos "sin tener que construir un mercado desde cero". Cada vez más empresas migran a estas estructuras para ampliar sus canales de comunicación con sus clientes, o apuestan al desarrollo de aplicaciones a partir de las herramientas ofrecidas por estos actores. Se amplía el grado de dependencia a estas plataformas que, como contraparte, se hacen de una mayor variedad y cantidad de datos.

Según Srnicek, el éxito de las plataformas radica en el efecto en red: "mientras más numerosos sean los usuarios que hacen uso de la plataforma, más valiosa se vuelve esa plataforma para los demás" (p. 46). Cuanta más gente use un producto o servicio, más valioso será para otros usuarios. Una persona que busca un producto ingresa en Amazon porque encuentra la mayor oferta de compras y marcas; alguien interesado en conectarse con su entorno o establecer nuevos vínculos sociales, se registrará en Facebook o Instagram ya que concentran millones de usuarios; si necesita buscar la dirección de un determinado lugar, accederá a Google que cuenta con millones de colaboraciones de otros usuarios. El valor de las plataformas que se dedican a la venta de publicidad, principalmente Google y Facebook, aumenta con el número de usuarios. Los anunciantes obtienen acceso a una base de consumidores más grande y, por lo tanto, a un tesoro mayor de datos de potenciales clientes. Hay una lógica en la que los usuarios generan más usuarios que buscan, compran, publican y contribuyen al caudal de datos que los algoritmos procesan para perfeccionar su performance. Así, el autor concluye que el mercado de las plataformas tiende naturalmente a la monopolización.

Scott Galloway reforzará esa idea al caracterizar a las plataformas como "empresas Benjamin Button" (2018, p. 146) que "envejecen en sentido inverso". A mayor tiempo de uso de una plataforma, más amplio el volumen de datos aportados por los usuarios y mejores las capacidades de procesamiento de los algoritmos que subyacen en la base de estas estructuras.

Ambos autores coinciden en que estas plataformas tienden a otro comportamiento que potencia los monopolios: la compra de proyectos innovadores que pueden llegar a poner en

jaque su posición dominante “gastando importantes montos de dinero para comprar otras empresas (…) se están convirtiendo en dueñas de las infraestructuras de la sociedad”(Srnicek, 2018, p.84). Las adquieren para incluirlas entre sus funcionalidades y también para cerrarlas o discontinuar los productos subyacentes (adquisiciones asesinas). El acceso superior a datos que tienen estas empresas, a través de su ingeniería y sus bases de millones de usuarios, hace que identifiquen y adquieran rivales al principio de su ciclo de vida, antes de que ninguna autoridad pública pueda identificar su rápido crecimiento y prohibir esa compra por ser anticompetitiva.

Galloway toma el caso de Snapchat, una plataforma que planteó una innovadora interacción de los usuarios a través de las imágenes. Las fotos desaparecen luego de una determinada cantidad de tiempo, generalmente a las 24 horas. Para Facebook, esta plataforma significaba un riesgo ya que Instagram también se basa en la interacción vía imágenes. En el 2013, luego de que el cofundador de Snapchat, Evan Spiegel, se negara a que la empresa fuera absorbida por Facebook por una oferta de tres mil millones de dólares, la red social comenzó a apropiarse de sus ideas y desarrolló las historias (stories). El autor metaforiza a la plataforma como “una serpiente pitón que se está tragando una vaca. A medida que la vaca va entrando, la serpiente adopta su forma. Una vez digerida, la serpiente vuelve a su forma original” (2018, p 152). El informe del Subcomité de Investigación de la competencia de los Estados Unidos expone que “menos de un año después de su introducción, las historias de Instagram tenían más usuarios activos diarios (200 millones) que las historias de Snapchat (161 millones)”[44]. Para el año 2018, el número se había duplicado.

El informe del Subcomité identifica un caso semejante con la aplicación de chat HouseParty que, luego de rechazar la oferta de adquisición por parte de Facebook, lanzó una nueva funcionalidad, “la sala de estar en internet” (p. 166). Esto hizo que unos meses después, Facebook actualizara su aplicación Messenger para ofrecer “salas de estar virtual”. Entre los años 2017 y 2018, la cantidad de usuarios activos de Houseparty se redujo a la mitad.[45]

El auge de la IA en la industria digital refuerza la tendencia del mercado a que el ganador se quede con todo como consecuencia de las economías de escala y los efectos de red. (Goldfarb, Trefler, 2018, p 8). ¿Qué significa hablar de economías de escala? A medida que aumentan las ventas, el costo unitario promedio disminuye. Una firma dominante puede extender su alcance a mercados adyacentes con sus propios productos sin costos altos. Si una empresa tiene suficiente experiencia técnica o acceso a vastos datos de consumidores, el costo de aplicar este recurso en un nuevo mercado es relativamente bajo. El gasto de desarrollar una actualización es bajo y tiene un impacto exponencial para millones de

[44] https://money.cnn.com/2017/04/13/technology/instagram-stories-snapchat/index.html
[45] https://www.businessofapps.com/data/houseparty-statistics/

usuarios de manera instantánea. Según el informe del Subcomité de Estados Unidos, “las plataformas obtienen más de los consumidores de lo que los consumidores obtienen de las plataformas” (p.45). A cambio de servicios "gratuitos", los usuarios proporcionan datos personales y metadatos sobre otros comportamientos más generales. Por ejemplo, al obtener la ubicación de un dispositivo, también se conoce el tráfico de la zona o los comercios que están cerca.

Otra característica que según el informe del Comité refuerza las lógicas monopólicas del mercado son los costos de cambio (p.42): qué debe resignar o perder un usuario si decide cambiarse a otra plataforma que ofrece un servicio similar. Es muy difícil exportar, descargar y luego subir masivamente toda la información que un usuario tiene en Facebook (publicaciones, interacciones sociales, imágenes no sólo propias sino en las que fue etiquetado) o en Google (historial de búsquedas, documentos de Drive, emails, reseñas y ubicaciones en Google Maps). En el caso de Amazon, un vendedor en línea que haya generado cientos de reseñas y calificaciones de productos no puede migrarlas a otra plataforma.

¿Qué efectos tienen todos estos factores sobre la innovación? En el 2014 las Startups cerraron 4255 contratos con inversores. En 2018, el número se redujo a casi la mitad (2.206)[46]. La tasa de emprendimientos (la cantidad de startups y firmas jóvenes) en la industria cayó del 60% en 1982 a 38% en el 2011[47].

El informe del Subcomité define al mercado de plataformas como una “zona de muerte” ya que hay una ausencia total de competencia: “los capitalistas de riesgo pierden el incentivo de invertir en nuevos participantes dispuestos a desafiar el dominio de las empresas establecidas mediante la competencia directa” (p. 37). Se trata de un escenario en el que “se compite para el mercado y no en el mercado” (p.13). Las empresas establecidas no se sienten presionadas para innovar, aumentar el nivel de los estándares de seguridad y calidad del servicio o garantizar la atención al usuario ya que no hay otros actores que hagan peligrar su posición dominante. Además, estas empresas están especialmente interesadas en la recopilación de los datos de los usuarios por el valor agregado que extraen de ellos, por lo que es poco probable que aboguen y trabajen para garantizar la privacidad de sus usuarios.

Facebook

¿Qué implica una posición dominante en el mercado de datos?, ¿cómo influye en los modos en los que se filtra la información a millones de usuarios? Durante la última década, las

[46] https://techcrunch.com/2019/03/16/decade-in-review-trends-in-seed-and-early-stage-funding/
[47] https://www.kauffman.org/wp-content/uploads/2019/12/declining_business_dynamism_in_us_high_tech_sector.pdf

técnicas de IA, combinadas con la hipersegementación de los públicos, tuvieron un impacto incluso en las estrategias de campañas electorales.

Estas tecnologías se utilizaron para direccionar y personalizar la difusión de mensajes políticos a través de redes sociales, tanto por medio de campañas políticas oficiales, como por noticias falsas y campañas de desinformación.

Uno de los casos más mediáticos fue Cambridge Analytica en el 2018. Los diarios The Guardian (Inglaterra) y The New York Times (Estados Unidos) revelaron una filtración de datos de millones de usuarios de Facebook utilizados para manipulación política. La empresa Cambridge Analytica difundía en Facebook una aplicación desarrollada por Michael Kosinsi, un científico de datos de la Universidad de Cambridge (cedida a Cambridge Analytica para que fuera empleada con fines puramente científicos). Esta aplicación ofrecía realizar un test de personalidad que sería parte de una investigación académica. Para poder completarlo, los usuarios daban consentimiento de acceso no sólo a sus datos, sino también a los de todos sus amigos de la red social. Se violaban las normas de uso de datos de Facebook vigentes en ese momento que impedían vender esos datos o usarlos para publicidad.

Christopher Wylie, exempleado de Cambridge Analytica, detalló que aunque sólo 270.000 personas habían dado el permiso explícito, llegaron a obtener información de 87 millones de usuarios de Facebook. Estos datos fueron procesados para influir en las campañas de políticos como Donald Trump y Ted Cruz, y en el Brexit en Gran Bretaña. Wylie confesó que "aprovechamos Facebook para recolectar millones de perfiles de usuarios. Y construimos modelos para explotar eso y apuntar a sus demonios internos"[48]. Luego de más de un año de investigaciones, la Comisión Federal de Comercio de Estados Unidos (FTC) sancionó a Facebook en julio de 2019 con una multa de US$5.000 millones de dólares por prácticas deshonestas en el manejo de la seguridad de los datos de sus usuarios.[49]

Mark Zuckerberg es dueño de Facebook, Instagram y Whatsapp. Controla el 95% del mercado en Estados Unidos.50 En el año 2012, Zuckerberg compró Instagram para aplacar a su principal competidor. En Estados Unidos, está prohibida la adquisición de una empresa rival que implique concentración excesiva de poder dentro de un mismo mercado. Sin embargo, la compra fue aprobada por el gobierno ya que se consideró que Facebook e Instagram no eran rivales directos: mientras que Facebook era considerada una red social, Instagram se concebía como una aplicación de fotografía.

Google

[48] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump
[49] https://www.bbc.com/mundo/noticias-49093124
[50] https://es-us.finanzas.yahoo.com/noticias/fundador-instagram-miedo-facebook-122002235.html

Según el estudio de la Autoridad de la Competencia del Reino Unido anteriormente citado, en julio de 2020 la empresa Google concentraba el 90% de las búsquedas que las personas realizan en la web. Esto convierte al buscador casi en la puerta de entrada a Internet. Sin ir más lejos, el verbo "googlear" se ha generalizado en la sociedad. En este mismo informe, se evidencia que Google absorbe más del 90% de los ingresos publicitarios. Martín Becerra destaca que "sus precios para el mercado publicitario son entre un 30 y 40 por ciento más altos que los de Bing (de Microsoft) al comparar términos de búsqueda similares. Facebook (...) generó más de la mitad de los ingresos publicitarios en redes sociales. A modo de comparación, su mayor competidor, YouTube (de Google) ganó "sólo" entre el 5 y el 10 por ciento"[51] .

En palabras de los fundadores de Google, Larry Page y Serguéi Brin, el objetivo inicial del buscador fue organizar la información del mundo para hacerla universalmente accesible y útil a través de múltiples aplicaciones. Por ejemplo, su navegador Google Chrome se ha convertido en el más utilizado a nivel mundial. Millones de usuarios autorizan el almacenamiento de sus contraseñas por comodidad y practicidad.

Según el sitio web de analítica de datos internacional Statcounter, en Argentina, entre octubre del 2019 y 2020, Google capturó alrededor del 97% de todas las consultas de búsquedas generales, seguido por Bing que sólo procesó el 0.13%. Sobre el total de búsquedas, desde computadoras de escritorio abarcó el 93%, mientras que desde dispositivos móviles llegó a monopolizar el 99% de las búsquedas.[52] En lo que respecta a navegadores, para el mismo período de tiempo, el 83% de los usuarios que ingresaron a Internet lo hicieron desde el Navegador Chrome, seguido de Firefox (4.53%), Safari (4.06%) y Edge (3%)[53].

Este gigante de Internet ya fue multado en varias ocasiones en la Unión Europea. Desde 2017, acumula un total de 8.250 millones de euros por sanciones:

- En marzo de 2019, la Comisión Europea acusó a la empresa de restringir el libre comercio a través de su servicio publicitario "Adsense for Search" que Google ofrece a las páginas web para añadir anuncios a su motor de búsqueda. Luego de una serie de investigaciones entre 2006 y 2016, se descubrió que la compañía incluía la firma de cláusulas de exclusividad y bloqueaba la publicidad de sus competidores, al ser el operador más fuerte en la intermediación de publicidad en la búsqueda en

[51] http://revistaanfibia.com/ensayo/tus-zonas-erroneas/
[52] https://gs.statcounter.com/search-engine-market-share/mobile/argentina
[53] https://gs.statcounter.com/browser-market-share/desktop/argentina

línea, “ostentando una cuota de mercado superior al 85% en el Espacio Económico Europeo durante la mayor parte de este período”.[54]

- ŏ En junio del 2017, la Comisión multó a Google por 2.424 millones de euros por ventajas ilegales a su propio servicio de compras “Google Shopping”. A través del uso de sus propios algoritmos, manipulaba el posicionamiento de sus competidores en los resultados de las búsquedas, que llegaban a aparecer en la cuarta página, muy poco visitada por los usuarios. La comisaria europea de la competencia de la Unión Europea declaró que “Google ha denegado a otras empresas la posibilidad de innovar y de competir según sus méritos. Y lo que es más importante, ha denegado a los consumidores europeos una auténtica oferta de servicios y todas las ventajas de la innovación”.[55]
- ŏ En julio de 2018, la Comisión Europea sancionó a Google luego de una investigación iniciada en el 2015 sobre su sistema operativo Android para dispositivos móviles. Para adquirir la licencia de Google Play Store Google exigía a los fabricantes de celulares la preinstalación de Google Search y su navegador Chrome. Además, fue acusado de pagar a grandes fabricantes para que preinstalaran de forma exclusiva Google Search en sus dispositivos y prohibir a los fabricantes de preinstalar aplicaciones de Google en dispositivos que funcionaran con otras versiones de Android no aprobadas por la empresa.[56] De esta manera, se desincentivaba la preinstalación de motores de búsqueda de otros fabricantes de teléfonos. Muchos competidores de Google tuvieron que retirarse del mercado de navegadores en dispositivos móviles. Actualmente el 90% del mercado de telefonía móvil se maneja con sistemas operativos desarrollados por Google o Apple con el IOS.

En la investigación llevada adelante por el Subcomité, se hace un análisis sobre cómo a lo largo de los años Google fue difuminando y haciendo cada vez más sutil la diferencia entre los resultados orgánicos, que son los que efectivamente surgen del término ingresado en el buscador, y los anuncios publicitarios. A través de estas prácticas, Google desvía tráfico a anunciantes que deben pagar por cada clic que se hace en sus enlaces. No todos los usuarios son capaces de discernir si los contenidos a los que accede son producto de su propia intención de búsqueda o si su recorrido está guiado por intereses comerciales. La forma misma a la que accede y navega en internet está condicionada por factores económicos. Además, Google aumenta la cantidad de anuncios que aparecen sobre los resultados de búsqueda: “la conducta de Google ha socavado la competencia, engañado a

[54] https://blog.cuatrecasas.com/competencia/google-adsense-multa-1490-abuso-dominio-publicidad-linea/#:~:text=Google%20AdSense%3A%20Multa%20de%201.490,dominio%20en%20publicidad%20en%20l%C3%ADnea&text=AdSense%20for%20Search%20funciona%20como,propietarios%20de%20sitios%20web%20editores.
[55] https://ec.europa.eu/commission/presscorner/detail/es/IP_17_1784
[56] https://www.infobae.com/america/tecno/2018/10/10/google-apela-multa-record-de-usd-4-991-millones-de-ue-por-android/

los consumidores y degradado la calidad general de los resultados de búsqueda (...) mientras permite a Google explotar aún más su monopolio sobre las búsquedas generales" (p. 197).

La prensa, en peligro

Google y Facebook hacen uso de los contenidos periodísticos en los resultados de sus búsquedas sin pagar ningún tipo de remuneración a los medios por los derechos de autor de esos contenidos. La posición de los medios en los últimos años se debilitó como consecuencia de que la publicidad, su principal sustento económico, migró a las plataformas online. En Estados Unidos desde 2006, los ingresos por publicidad en los medios tradicionales (que son esenciales para financiar periodismo de alta calidad) cayó más del 50%[57]. En junio del 2020, la asociación News Media Alliance, que reúne alrededor de 2.000 diarios de EEUU y Canadá, publicó el informe "White Paper"[58] en el que denuncia que Google se aprovecha del contenido de las noticias en su beneficio. Lo acusa de haberse convertido en "un editor en sí mismo" ya que muestra la información en estructuras enriquecidas y visuales. Los medios de comunicación le aportan los contenidos que indexa cuando un usuario realiza una búsqueda en su motor. Como contraparte, Google no paga a los medios ningún tipo de remuneración por el uso de esa información que la empresa utiliza como recurso para mezclar con publicidad. Google argumenta que compensa al autor de los contenidos al generar tráfico a la información que los medios producen.

En este White Paper, los medios piden que se debata una ley que preserve a los medios de comunicación, y se les habilite un período de negociación de 48 meses para que toda la prensa puesta de acuerdo pueda solicitarle a Google una compensación económica.

En julio de 2020, Australia presentó un proyecto de ley sin precedentes en el que busca obligar a Facebook y Google a pagar a los medios por incluir sus contenidos entre los resultados de sus búsquedas. Este "código de conducta restrictivo" también considera el "acceso a los datos de los usuarios, la transparencia de los algoritmos y el orden de aparición en los flujos de información de las plataformas y los resultados de búsqueda"[59] .

En la última década, en Australia se perdieron alrededor de 3.000 puestos de trabajo en la prensa. Según John Frydenberg, ministro australiano de finanzas, "por cada 100 dólares australianos gastados en publicidad online, excluyendo los anuncios por palabras, casi un tercio va a Google y Facebook". Este proyecto de ley incluye una cláusula que prohíbe cualquier tipo de discriminación en el tratamiento de la información de los medios australianos. Se busca prevenir lo ocurrido en Europa luego de que grandes grupos

[57] https://www.bloomberg.com/opinion/articles/2018-06-01/goodbye-newspapers-hello-bad-government
[58] http://www.newsmediaalliance.org/wp-content/uploads/2020/06/Final-Alliance-White-Paper-June-18-2020.pdf
[59] https://www.eltribuno.com/jujuy/nota/2020-8-1-11-31-0-australia-hara-que-facebook-y-google-paguen-por-el-contenido-de-los-medios

editoriales de Alemania, Francia y España exigieran la aprobación de leyes nacionales en defensa de los derechos de autor. Como represalia, Google dejó de incluir en sus resultados de búsqueda las noticias de ciertos medios europeos para que el acceso a los contenidos de estos sitios se desplomara.

A pesar de que Facebook y Google funcionan como intermediarias de noticias en línea y definen el flujo de noticias a los acceden millones de usuarios, no se conciben como medios de comunicación ya que eso implicaría asumir un rol de mayor responsabilidad respecto de la información que circula a través de ellos. Deberían tener en cuenta "la objetividad editorial, la comprobación de datos, la ética periodística, el discurso políticamente correcto" (Galloway, 2018, p. 165). Facebook y Google eligen ganadores y perdedores a través de algoritmos que incrementan o quitan visibilidad y tráfico que puede destruir pequeños medios. No invierten en producción de noticias y no tienen responsabilidad por su calidad y precisión. Además, el hecho de considerar a Google o Facebook como editores de contenidos, implicaría plantear el riesgo a la libertad de expresión o censura previa sobre la decisión de incluir o no cierta información en interfases en las que acceden millones de usuarios.

Apple

Apple fue denunciada por prácticas monopólicas llevadas adelante en su tienda Appstore, que permite descargar aplicaciones a los dispositivos móviles de la marca, iPhone, iPad, Apple Watch, el iPod y Apple TV. Esta plataforma ha generado desde 2008 más de 155.000 millones de dólares en beneficios para terceros, convirtiéndose en la tienda más rentable de la historia.[60]

La polémica se desató en marzo de 2019 por un reclamo que la empresa Spotify, sistema líder de streaming musical sueca, presentó a la agencia antimonopolio europea. Se denunciaba que existía una serie de requisitos que favorecían a Apple Music por sobre sus competidores. La denuncia enumera varias prácticas abusivas:

- Apple exige a las compañías el pago de un impuesto del 30% por utilizar su sistema de pago, lo que incrementa los precios de los servicios a los usuarios.
- Prohíbe incluir botones de compra o enlaces a promociones, a diferencia de la plataforma de Google. Spotify dejó de utilizar el sistema para suscribirse al servicio, por lo que los usuarios no podían acceder a la suscripción directamente desde el iPhone o iPad, sino que debían hacerlo desde un navegador portátil.
- Denunciaron que Siri, el asistente inteligente de los dispositivos Apple, no se entiende con su aplicación. También detectaron incompatibilidades de la aplicación

[60] https://www.elconfidencial.com/tecnologia/2020-07-29/app-store-competencia-acusaciones-monopolio_2698184/

con el reloj de la marca (Apple Watch) que genera errores recurrentes en sus funcionalidades.

- Existen retrasos en las actualizaciones de las aplicaciones por al proceso de revisión que lleva adelante Apple. Muchos errores de funcionamiento, que pueden incluir la vulneración de los datos de los usuarios, pueden demorarse más tiempo en ser solucionados.

La App Store de Apple es el único medio para distribuir software en dispositivos IOS. Google Play Store es la tienda de aplicaciones dominante en dispositivos Android. Google permite a los usuarios descargar tiendas de aplicaciones alternativas, aunque nunca llegan a contar con la oferta de aplicaciones de las tiendas líderes. Los desarrolladores de aplicaciones que quieran llegar a todo el mercado deben tener una aplicación tanto en la App Store como en la Play Store.

Como el negocio de las tiendas de aplicaciones se concentra en Apple y Google, tienen el poder de determinar los términos y condiciones que los desarrolladores de aplicaciones deben aceptar para distribuir su software.

Amazon

Su plataforma de compra-venta de productos es acusada de recopilar información de las empresas y comercios que la utilizan: los volúmenes de venta, precios y hasta sus estrategias empresariales en base a la interacción y actividad de los usuarios.

Con toda esta información, Amazon analiza qué productos pueden ser redituables y comienza a producirlos y venderlos en sus líneas AmazonBasics y Amazon Essentials. Los ofrece a precios predatorios (por debajo de los costos) y destruye a la competencia. Además, invierte millones de dólares al año en logística y medios de entrega para garantizar que el producto llegue en tiempo récord y se constituya como una de las empresas más confiables de comercio online: “en 2015, Amazon tuvo un gasto de siete mil millones de dólares en tarifas de envío” (Galloway, 2018, p. 58), un gasto que los comercios minoristas o empresas de e-commerce más pequeñas no pueden considerar.

Ya en 2017, con el lanzamiento de Amazon Essentials, desde la empresa habían reconocido que “analizan los comentarios de los consumidores para crear los productos de alta calidad, cómodos a un precio accesible”[61] al considerar que los clientes mejoran los productos a través de sus comentarios en la plataforma.

Uno de los casos en los que Amazon aplicó estas prácticas es el de los pañales Diapers.com[62], un sitio de la empresa Quidsi, dedicada a la venta online de pañales y

[61] https://www.merca20.com/amazon-confirma-lo-que-ya-sabiamos-utilizo-los-datos-de-sus-clientes-para-optimizar-marcas-propias/

[62] https://elceo.com/tecnologia/amazon-comparecencia-jeff-bezos-congreso/

productos para bebés. Amazon detectó un importante volumen de ventas de la empresa que se expandió al mercado de otros productos en una nueva página web (soap.com). Un año después, Amazon lanzó al mercado una línea de productos para bebés, "Amazon Mom", que ofrecía hasta un 30% de descuento a los usuarios que se suscribieran para recibir sus ofertas de manera mensual por suscripción. Este nuevo negocio llegó a representar para Amazon una pérdida de hasta 200 millones de dólares en pañales[63], pero le permitió comprar Quidsi por alrededor de 500 millones de dólares y cerrarla en 2017.

Tal como se explicó en el capítulo 1, otro servicio que ofrece Amazon es el de Amazon Web Servicies (AWS). Srnicek define este tipo de plataforma como "de la nube" y consiste en "alquilar servicios informáticos de la nube, que incluyen mantenimientos on-demand de servidores, almacenamiento y potencia para ordenadores, desarrollo de software y aplicaciones listas para usar (2018, p 60). De esta manera, Amazon tiene acceso no sólo a las estrategias de mercado o productos de las empresas sino también, al propio código, a la arquitectura de los desarrollos informáticos que aloja. Aquellas empresas o personas que hacen uso de estos servicios no tienen muchas alternativas en materia de prestadores (el costo de desarrollar estas tecnologías de cloud computing es muy alto). Toda la información que se almacena en la nube es poco interoperable con otros sistemas, por lo que las consecuencias de abandonar este servicio pueden llevar a perder información, además de los costos de salida que Amazon exige pagar a sus clientes cuando abandonan la plataforma.

Antecedentes de monopolios en Estados Unidos

La conformación de monopolios en mercados de bienes y servicios emergentes no es una novedad de la sociedad de la información. En Estados Unidos, existen la Clayton Act y la Sherman Act que buscan garantizar y defender la competencia y el bienestar de los consumidores.

En el desarrollo de las comunicaciones, se puede destacar el caso de AT&T (American Telephone and Telegraph Company), resultado de la fusión de tres empresas en 1899. Se constituyó como un monopolio de hecho que controlaba las llamadas locales, internacionales y de larga distancia, además de producir los equipamientos telefónicos. Tal como lo describe Aguiar "era la empresa de comunicaciones más grandes del mundo, llegando a valer 150.000 millones de dólares en 1984" (2007, p. 226).

Para la prestación de llamadas de larga distancia, surgieron otras empresas como Sprint y MCI. Esta última acude a la Secretaría de Comercio para denunciar que la posición dominante de AT&T en el mercado no permitía el desarrollo de competidores. Los usuarios

[63] https://arstechnica.com/tech-policy/2020/07/emails-detail-amazons-plan-to-crush-a-startup-rival-with-price-cuts/?comments=1

no tenían libertad de elección y había un único actor que fijaba precios altos en las llamadas de larga distancia.

La telefonía no estaba definida legalmente como monopolio natural o de derecho, sino que se había constituido como un monopolio de hecho. En 1984, el Juez Haroldo Greene falló que AT&T debía vender su negocio de telefonía local a siete empresas diferentes que no podían tener nada que ver entre sí ni con AT&T, conocidas como las Baby Bells. La multiplicidad de actores en el mercado de la telefonía permitió crear un entorno competitivo que bajó el precio de las llamadas y, por lo tanto, beneficio a los usuarios.

¿Qué sucede en el escenario contemporáneo de las GAFA? Definitivamente, no se trata de un monopolio natural o de derecho ya que no existe legislación alguna que apruebe o defina la presencia de uno o pocos actores en el negocio de las plataformas digitales, ni tampoco se exige el cumplimiento de metas definidas. No se trata de un mercado en el que lo más racional sea la prestación de un servicio por parte de un único actor. Al contrario, cuantos más agentes participen en el mercado, mayor será la oferta en originalidad de propuestas, estándares de calidad e innovación para atraer a más usuarios a sus plataformas. Una brecha de seguridad en las bases de datos de una empresa tendría un impacto irreversible si se tratara de un mercado competitivo, ya que los usuarios podrían optar por otra plataforma con mejores estándares de seguridad. Pero como los costos del cambio a otra plataforma pesan y no hay alernativas que concentren tal cantidad de información, no hay un movimiento dinámico de los usuarios en sus entornos virtuales.

¿Puede hablarse de un monopolio de hecho? Estas cuatro empresas dominan el mercado de datos, la venta por internet, deciden qué contenidos se muestran a los usuarios y son la puerta de entrada a Internet a través de navegadores, sistemas operativos y buscadores que ellos mismos desarrollan. Sus márgenes de ganancias y, por lo tanto, su capacidad de inversión en el desarrollo tecnológico hacen muy difícil la puerta de entrada a nuevos actores o StarUps. Si surgen actores que pongan en peligro su posición dominante, son absorbidos por alguna de estas empresas. La posibilidad de que el mercado se abra naturalmente a la competencia es un escenario poco probable. Cabría plantear cuáles serían los efectos de un fallo como el del año 1984.

Posibles recomendaciones de regulación

El Subcomité de Derecho Antimonopolio, Comercial y Administrativo de los Estados Unidos incluye en el capítulo VI de su informe una serie de recomendaciones para repensar la regulación de las plataformas en el mercado de la economía digital en pos de la competencia. Propone reformar la legislación en el marco de los siguientes ejes:

1. **Restaurar la competencia en la economía digital:**

a. Establecer separaciones estructurales a partir de las cuales se prohíbe que una empresa dominante opere en mercados en el que es, al mismo tiempo, intermediario y compite con terceros que dependen de su infraestructura. Por ejemplo, Amazon es a la vez la plataforma para que terceros vendan sus productos, y también oferente de sus propias líneas de productos y servicios, que compiten directamente con los productos de los usuarios que utilizan la plataforma para vender.
b. Restricción en líneas de negocios adyacentes que limitan los mercados en los que pueden actuar estas empresas dominantes. En el caso de Google o Facebook, hacen ingeniería de datos para identificar cuáles son las aplicaciones emergentes más utilizadas para reconocer posibles competidores. Una vez detectados, actúan sobre ellos, ya sea adquiriéndolos o copiándose de sus funcionalidades para reducir el tráfico de usuarios a la aplicación. Lo mismo ocurre con Amazon que además de brindar servicios de cloud computing, y ser plataforma para compra y venta de productos, se expande hacia ramas de producción y venta de productos y servicios minoristas que identifica como redituables.
c. Requisitos de no discriminación que prohiben a las plataformas dominantes configurar sus algoritmos y sus exigencias para ofrecer sus productos en detrimento de otros (autopreferencias). Se busca exigir que las plataformas ofrezcan a terceros sus servicios en igualdad de condiciones para que no tengan la capacidad de elegir ganadores y perdedores. Por ejemplo, Google no podría exigir a los fabricantes de teléfonos que preinstalen sus aplicaciones para otorgar la licencia de Android. Quedaría prohibida también la configuración predeterminada de los servicios de Google Search como buscador, Google Maps como Navegación. Además se debería hacer más amigable y visible el menú que permite modificar estas configuraciones en los dispositivos.
d. Interoperabilidad y portabilidad de datos: las plataformas dominantes deben hacer sus servicios compatibles con otros prestadores para permitir que, en caso de que el usuario quiera migrar a otra plataforma, pueda exportar su información en formatos que permitan ser fácilmente cargados. Actualmente en el caso de Facebook, el usuario puede descargar su información pero se exporta en formato .zip o pdf que los hacen poco migrables. No puede mucho más que cargar sus fotos en alguna plataforma de imágenes. Todo lo que implica información de su gráfico social (interacciones con amigos, grupos,

publicaciones) no es plausible de ser publicado en otra red de manera masiva y directa.

e. Prohibición de futuras fusiones y adquisiciones por parte de las plataformas dominantes. El subcomité recomienda que el Congreso considere que "cualquier adquisición por parte de una plataforma dominante se presumirá anticompetitiva a menos que las partes de la fusión puedan demostrar que la transacción es necesaria para servir al interés público y que no se pueden lograr beneficios similares a través del crecimiento y expansión internos" (pp. 389).
f. Abrir un espacio de diálogo obligatorio para que emisoras y editores negocien colectivamente con las plataformas monopólicas un tratamiento equitativo de la información.
g. Prohibir los abusos de poder en negociación superior a través de protecciones para personas y empresas: al ser las únicas empresas que los usuarios pueden elegir, las plataformas pueden imponer condiciones de uso abusivas del tipo "tómalo o déjalo" que implican un tratamiento de una mayor cantidad de datos personales, apropiación de secretos comerciales o contenido patentado de las empresas.

2. Fortalecimiento de las leyes antimonopolio:

a. Estados Unidos cuenta con un sólido andamiaje legal en materia de antimonopolios. Uno de los grandes pilares es el valor que se le concede a la competencia como garante de la democracia y la economía. Entre las principales leyes en la materia se encuentran la Ley Sherman (1890), Ley Clayton (1914), la Ley de la Comisión Federal de Comercio (1914), Ley Robinson-Patman de 1936, la Ley Celler-Kefauver de 1950 y la Ley Hart-Scott-Rodino de 1976. El Subcomité denuncia que la Corte Suprema adoptó una postura que considera que la aplicación deficiente de leyes antimonopolio es preferible a la aplicación excesiva (p.393). Recomienda reformas legislativas que reviertan esta conducta en los mercados digitales.
b. Fortalecer la Sección 7 de la Ley Clayton que prohíbe cualquier transacción que reduzca sustancialmente la competencia o prepare el terreno para un escenario de monopolio.
c. Reglas claras y presunciones estructurales para fortalecer la Sección 2 de la Ley Sherman que establece que es ilegal: "monopolizar, o intentar monopolizar, o combinar o conspirar con cualquier otra persona o personas, para monopolizar cualquier parte del comercio o el comercio entre los

distintos Estados"[64]. A partir de una presunción estructural, estarían prohibidas todas las transacciones que le adjudiquen a una única empresa el control de una porción muy extensa de un mercado particular o favorezcan la concentración, así como también aquellas que neutralicen potenciales rivales. Las empresas deberían mostrar pruebas de que la fusión no afectaría a la competencia.

Reflexiones

Estas pocas empresas filtran los contenidos que consumen millones de personas día a día. Los usuarios no suelen ser conscientes de los criterios que priorizan ciertas publicaciones sobre otras. Tal como sucedió con el escándalo Cambridge Analytica, las empresas ceden sus datos a centenares de terceros. Empresas que por ejemplo, se dedican a la comunicación política y detectan blancos posibles para suministrar contenidos dirigidos. Estas prácticas impactan directamente sobre la calidad democrática.

En Argentina, la publicidad en los medios tradicionales está regulada de forma tal que todos las fuerzas políticas cuentan con espacios distribuidos de manera equitativa. Este tipo de regulaciones aún no está presente en las redes sociales, en las que la inversión en espacios publicitarios no está limitada. Esta capacidad ilimitada de alquiler de espacios da lugar a un escenario de desigualdad de condiciones entre los partidos con más recursos para invertir en las plataformas y los que no pueden hacerlo o no cuentan con el personal capacitado en lo digital para llevarlo a cabo.

La concentración en el mercado de datos afecta de lleno en la libertad de expresión. ¿Las plataformas deben ser responsables por el contenido que circula a través de ellas? Si la respuesta es sí, ¿está bien que tengan el poder de decidir qué contenidos se muestran y cuáles no?, ¿no podría considerarse como una censura previa?, ¿qué criterios hacen que un contenido publicado por un usuario en una red sea dado de baja?, ¿quién define esos criterios?, ¿puede una plataforma censurar a un usuario de manera indefinida?

Los usuarios acceden a información filtrada por algoritmos, cajas negras que muchas veces ni las propias empresas pueden explicar su funcionamiento. "La IA es incapaz de distinguir las noticias falsas, como mucho puede llegar a sospechar cuáles lo son, en función de su origen. Solo verificadores humanos pueden determinar si una noticia es falsa o no" (Galloway, 2018, p 171). Aunque se empleen personas para moderar contenidos, ¿qué se toma como verdad?, ¿bajo el lente de qué actores se define qué es la verdad o qué publicación es de mal gusto? Si la decisión está en manos de empleados de empresas privadas como Facebook o Google ¿qué garantiza que haya diversidad de pensamientos en las plataformas? Si efectivamente una publicación se da de baja en una plataforma por ser

[64] Ley Sherman Antitrust (1890) https://eprints.ucm.es/54581/1/5329913994.pdf

falsa, ¿qué impacto tiene en las millones de personas que efectivamente pudieron acceder al contenido antes de fuera inhabiiltado?

Por otro lado, si no se aplican legislaciones para regular este mercado, la posibilidad de generar competencia es nula. Por ejemplo, los usuarios hace más de una década que aportan su información a Facebook. Una Startup jamás contará con esos diez años de datos y, por tanto, no podrá generar preferencias, posibilidades de perfilamiento ni contenidos a medida con tal grado de exactitud. Tal como puntualiza Galloway: "Ningún otro medio en la historia ha podido combinar la enorme escala de Facebook con su habilidad para individualizar el objetivo. Cada usuario ha creado su propia página y la ha ido llenando de contenido personal durante años" (2018, p. 137).

¿No es hora de revisar el desarrollo legal aplicado en los canales de comunicación previos a las plataformas para extrapolarlo a este mercado? Por ejemplo, en la telefonía fija o móvil los usuarios pueden intercambiar llamados aunque los operadores que les presten el servicio sean diferentes. Esto es posible gracias a la Interconexión que en Argentina está contemplada y regulada en el decreto 764/2000 de desregulación de los servicios. En el anexo II del decreto, conformado por el Reglamento Nacional de Interconexión (RNI), se define a la Interconexión en el Artículo 4 como "conexión física y funcional de las redes de telecomunicaciones utilizadas por el mismo o diferentes Prestadores, de manera que los clientes y/o usuarios puedan comunicarse entre sí o acceder a los servicios de otros Prestadores"[65]. La Interconexión resulta esencial para permitir la entrada de nuevos operadores de telefonía en las diferentes zonas geográficas. Garantiza la interoperabilidad de los servicios y la presencia de más de un prestador para la fijación de precios, el estímulo a la competencia y la innovación. ¿Qué sucede en el mercado de las redes sociales? ¿Whatsapp o Facebook no deberían ser interoperables con otras plataformas? Un usuario de Whatsapp sólo puede comunicarse con otra persona a través de esta misma aplicación. ¿No debería existir la posibilidad de hacer interoperables los mensajes o llamados o videollamdas con los de Telegram o cualquier otra aplicación de comunicación? Estos escenarios condicionan a los usuarios a que tengan que usar la misma plataforma ya que la mayoría de sus contactos está ahí. Lo mismo sucede en el caso de Facebook: sólo se puede acceder a la interacción con amigos que están en la misma red social o, en todo caso, en Instagram que es parte de la misma familia de empresas. En los entornos digitales, la interconexión no implicaría tener que incurrir en cuantiosos gastos para las empresas ya instaladas porque no se deben construir nuevas infraestructuras físicas, cableados o contratar personal especializado: son los mismos equipos de desarrollo los que deberían modificar los códigos y las arquitecturas digitales para permitir la interoperabilidad de

[65] Decreto 764/2000. Desregulación de los servicios. Reglamentos de Licencias para Servicios de Telecomunicaciones, Nacional de Interconexión, General del Servicio Universal y Sobre Administración, Gestión y Control de Espectro Radioeléctrico. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64222/norma.htm

plataformas. Así, las nuevas plataformas podrían participar de los entornos ya conocidos, beneficiarse de los efectos en red y enriquecer la oferta de funcionalidades y atractivos para los usuarios.

Si el volumen de estas pocas empresas no permite el desarrollo de nuevos competidores, se ha conformado un monopolio de hecho. Si es tan evidente que este mercado no podrá abrirse naturalmente a la competencia, ¿por qué las autoridades regulatorias no tomaron medidas para actuar sobre estas lógicas en un mercado tan sensible? Es difícil encontrar una única explicación, pero existen factores que influyen sobre la regulación estática.

En primer lugar, hay que tener en cuenta que estas empresas tienen un poder de lobby sin precedentes. En el informe del Subcomité se reconoce que "el crecimiento del poder de mercado de las plataformas ha coincidido con un aumento de su influencia en el proceso de formulación de políticas" y hace referencia a un "circuito de retroalimentación: más dinero gastado en cabildeo puede generar mayores retornos de acciones y participación de mercado, lo que, a su vez, puede estimular más cabildeo" (pp. 75). Hace referencia a donaciones que Facebook, Google y Amazon realizaron al American Enterprise Institute (AEI) y al Global Antitrust Institute de la Universidad George Mason, instituciones encargadas de defender la calidad de competencia del mercado: "al financiar a académicos y grupos de defensa, las plataformas dominantes pueden expandir su esfera de influencia, dando forma a cómo se gobiernan y regulan" (p. 76). No sólo se trata del poder economic: los Estados mismos utilizan las plataformas para su propio funcionamiento, por ejemplo, para la publicidad de sus políticas como parte de las estrategias de comunicación y el uso de servicios en la nube para almacenar información. Amazon Web Servicies presta servicios de cloud computing para el sector público. En el sitio web principal de AWS, la empresa afirma que trabaja con más de 6500 agencias gubernamentales sólo en Estados Unidos.[66]

Según el informe anteriormente citado, desde el año 1998, las GAFA, han adquirido en total 500 empresas, sin que las autoridades hayan bloqueado ninguna transacción por cuestionar la limitación en el mercado que eso significaría. Se trata de una preocupación que el mismo Subcomité de Derecho Antimonopolio, Comercial y Administrativo plantea. Aboga por un cambio ya que "al buscar acuerdos adicionales en inteligencia artificial y en otros mercados emergentes, las empresas dominantes de hoy podrían posicionarse para controlar la tecnología del mañana" (pp. 389). Hay que considerar que estas empresas desarrollan e invierten en el desarrollo de Inteligencia Artificial. Un claro ejemplo es la tecnología de reconocimiento de voz incluida en dispositivos móviles, parlantes y, sobre todo en los últimos años, en aparatos del hogar. Estas tecnologías no sólo registran las interacciones de voces del usuario, sino también conversaciones en segundo plano, entre los que puede haber niños. Se plantea toda una serie de desafíos en materia de privacidad frente a una

[66] https://aws.amazon.com/es/government-education/government/

tecnología cada vez más impregnada en las rutinas de las personas y en su propia intimidad.

En segundo lugar, la complejidad inherente de los algoritmos hace que carezcan de claridad técnica y transparencia que permita la auditoría por parte de las autoridades. Ni los propios directores de estas empresas pueden explicar el funcionamiento de los algoritmos detrás de sus prácticas. Poder entender su funcionamiento y sobre todo, detectar maniobras anticompetitivas como la autopreferencia, implica contar con las herramientas técnicas y el conocimiento para hacer un análisis pertinente que funcione como prueba de intencionalidades deshonestas.

Por último, existen factores geopolíticos que pesan en el margen de acción de los reguladores. Separar estas empresas o someterlas a un control que reduzca su ritmo de crecimiento puede hacer que pierdan relevancia y protagonismo no sólo a nivel nacional sino mundial. ¿En qué posición quedarían respecto de la expansión creciente de las plataformas de China? No hay que olvidar que en ese país también hay un mercado digital concentrado y manejado por el propio Estado que, lejos de abogar por la competencia, se apoya en la concentración para afinar y perfeccionar los recursos de vigilancia de su sociedad.

¿Estas empresas podrían haber surgido en entornos monopólicos como al que ahora está sometida la economía digital?,¿no podría haber otros Jeff Bezos, Mark Zuckerbergs con ideas más innovadoras, más ricas?, ¿el mundo llegó a su máxima expresión informática con estas plataformas?

Detrás de estas prácticas monopólicas, hay pequeñas empresas, negocios locales, emprendedores, puestos laborales que están en peligro. Quedan a merced de actores infranqueables que pueden decidir “bajarles la palanca” dentro de sus interfaces, borrándolos del territorio por el que circulan miles de millones de usuarios. El mundo digital, no es nada más ni nada menos que una arquitectura de código en pocas manos. Estos pocos deciden por qué calles puede (y debe) circular más gente, qué negocios deben ocupar más o menos lugar en el espacio público, pueden “cortar una calle” para que no se transite o ni siquiera se perciba como un camino alternativo, planifican con quién el usuario se va a cruzar por la calle con más o menos frecuencia, qué anuncios van a colarse en su camino y a qué información accede para construir su concepción de mundo y los acontecimientos que lo rodean. Un espacio público digital que cada vez tiene menos de público y colectivo, y más de intereses privados que conducen a los usuarios por atajos funcionales a sus propios intereses.

“El algoritmo, ¿el nuevo Hombre de Vitruvio?”

Los usuarios se han convertido en productores de datos que, en interacción, permiten arrojar luz sobre prácticas, preferencias y fenómenos sociales. Pero, ¿son los datos la versión más acabada de nosotros mismos?

Esta nueva revolución industrial, o mejor dicho, esta nueva era tecnológica, implica un cambio radical en las prácticas y los procesos sociales. El primer paso para actuar de manera crítica sobre la nueva realidad es entender los fenómenos que nos rodean cuando nos conectamos, tomamos decisiones y accedemos a la información. Los debates en torno a la transparencia, la privacidad y la libertad de expresión no surgen de la tecnología en sí misma, sino de su interacción con el complejo entramado de relaciones sociales, en cómo las personas se apropian de los desarrollos tecnológicos. Al hablar de Inteligencia Artificial, la primera imagen que invade el imaginario es la de un robot capaz de actuar como un ser humano, y que dominará el mundo. Llegó el momento de abandonar esa idea revolucionaria, de dejar de esperar ese cambio violento de una entidad que reemplazará a la humanidad: no tenemos aún robots pero sí GPS, redes sociales, plataformas de videollamadas. La tecnología no viene a dar vuelta la sociedad de un día para otro, sino que penetra sutilmente en los comportamientos de la sociedad, modificándola casi de manera silenciosa.

Las nuevas tecnologías no pueden provocar que la sociedad abandone de cuajo sus costumbres y prácticas tradicionales, pero tampoco puede permanecer ajena al avance tecnológico. Debe entender los mecanismos a partir de los cuales se obtienen cifras, se procesa la información y los riesgos que amenazan su privacidad.

Gran parte de la vida de las personas se desenvuelve en el mundo digital. Un territorio construido sobre hectáreas interminables de código que guardan y se asientan sobre miles de millones de datos de la sociedad. Grandes empresas y estados disputan por colonizar este territorio a través del uso del “nuevo petróleo”. Estudian a fondo los comportamientos humanos para pulir una maquinaria informática que logre captar la atención de los usuarios, los atraiga a pasar más tiempo en este mundo y generen así más datos, que refuercen el proceso de retroalimentación de un sistema que vende y controla a los usuarios. Se establece así un círculo vicioso conformado por más datos en manos de pocos que generan más conocimiento sobre los públicos y desarrollan más estímulos para que millones de usuarios pasen más tiempo en sus aplicaciones.

Las pocas empresas y estados más fuertes sobre las se asienta el desarrollo de la economía digital cuentan con enormes capitales para la innovación en un terreno en el que se manejan libremente, allanan la competencia adquiriéndola o clonándola para destruirla. Concentran recursos humanos y conocimiento que se internalizan en complejos sistemas de cómputo y procesamiento: maquinarias construidas a través de algoritmos específicos y

fragmentados en centenares de partes. Piezas de un rompecabezas de una caja negra cada vez más efectiva pero menos explicable.

La sociedad se mueve en un mundo que evoluciona a pasos agigantados, con tecnologías que no entiende cómo funcionan, que no están debidamente reguladas, pero de las que debe depender para llevar adelante su vida social, laboral, académica. Tal como afirma Langdon Winner “si la experiencia de la sociedad moderna nos muestra algo, es que las tecnologías no son simples medios para la actividad humana, sino también poderosas fuerzas que actúan para remodelar dicha actividad y su significado”(2008, p.39). Detrás del “sonambulismo tecnológico” que promete facilitar la vida de la humanidad, hay millonarios intereses económicos y políticos que están interesados en mantener a la sociedad sumida en el sueño de la utopía de un mundo más igualitario, rico y colectivamente construido, esa antigua promesa de Internet.

Las ciencias sociales deben tomar parte en esta nueva reconfiguración total de las estructuras sociales. Pero no deben hacerlo desde un lugar instrumental o reactivo. Esa postura las deja kilómetros detrás de la tecnología que continuamente cambia el terreno social. Deben analizar los fenómenos sociales para anticiparse, para plantear nuevos paradigmas que influyan en las políticas reales, que actúen ante los desafíos de acceso a la información, las brechas sociales, las nuevas relaciones de poder que amenazan los márgenes de decisión, las ideologías en pugna, el riesgo a la manipulación, los sesgos inherentes a la naturaleza humana, los abusos de las empresas y de los Estados en la vigilancia de sus poblaciones. Deben intervenir en la creación de marcos regulatorios capaces de equilibrar la libertad de expresión y transparencia con el derecho a la intimidad y privacidad, la libertad de competencia sin limitar la innovación. La sociedad no se define por las leyes de mercado, sino que el mercado debe adaptarse a las dinámicas sociales. Pero esto sólo se logra si hay investigación que anticipe las nuevas lógicas, la concentración de pocos actores, la construcción de nuevos colectivos y desigualdades.

Se habla de la “necesidad de regular a las empresas”, se critica el problema de los datos y de la privacidad de las grandes compañías, se señala la falta de conciencia o pasividad de los usuarios o los gobiernos frente a estas cuestiones. Sin embargo, si se contempla en el análisis la dimensión económica, el almacenamiento y procesamiento de los infinitos cúmulos de datos generados por los usuarios implican millonarios gastos para las empresas. Las nubes y otros recursos técnicos se apoyan sobre complejas infraestructuras que deben ser creadas, mantenidas y mejoradas constantemente.

Los usuarios optan por usar las versiones gratuitas de toda herramienta virtual que utilizan en su vida diaria. La sociedad hoy consume, gestiona y distribuye una cantidad de información como nunca antes, apoyándose sobre la gratuidad de producción de contenidos: editamos, diseñamos, escribimos, publicamos, trabajamos colaborativamente,

estudiamos, nos conectamos por videollamadas. Cabría preguntarse entonces qué pasaría si como consecuencia de la regulación, las empresas comenzaran a cobrar por los servicios que nos prestan. Es decir, se acotarían los márgenes de almacenamiento y uso de nuestros datos para la publicidad pero, como contraparte, los servicios gratuitos serían muy limitados y los aranceles por su uso deberían ser abonados por los propios usuarios. Si las empresas entienden que la mayoría de los usuarios no quieren pagar por lo que usan, seguirán ofreciendo sus servicios a cambio de los datos. La pregunta es: ¿hay que operar sobre los usuarios para explicarles que no pagar por un servicio equivale a estar dispuesto a ceder privacidad?, ¿hay que operar sobre las empresas que no fueron transparentes al momento de ofrecer la herramienta sin costo alguno, sin explicar que, en realidad, acceden a nuestra información porque les resulta valiosa?, ¿hay que analizar qué es lo que los gobiernos no hicieron a tiempo para frenar a estas empresas?

La Inteligencia Artificial ha llegado para quedarse y evolucionará exponencialmente. Potenciará las capacidades de unos pocos para acceder a más datos, filtrar más contenidos, diseñar publicidad más segmentada, vigilar a la población de manera más selectiva. ¿Cómo se puede revertir el proceso para empoderar a la ciudadanía, la democracia y el acceso a la información? Entender la Inteligencia Artificial significa entender el pensamiento y el comportamiento humano. Implica comprender cómo aprende la humanidad para extrapolarlo a modelos y reglas. Una humanidad que tiene pasiones, defectos, ambiciones, enigmas, errores y aciertos que las ciencias hasta el día de hoy todavía intentan desentrañar. ¿Puede un algoritmo representarnos como sociedad? Esa respuesta aún no se encuentra ni en el buscador de Google.

Bibliografía

Aguiar, H. (2007). *El futuro no espera*. La crujía ediciones.

Ascencio, L. y Gonzalez-Ramirez, R. (2018). Infraestructura portuaria en 2035. En G. Beliz (Ed.), *Algoritmolandia* (pp. 157-167). Planeta

Bishop, C. (2006). Reconocimiento *de patrones y Machine Learning*. Springer. http://users.isr.ist.utl.pt/~wurmd/Livros/school/Bishop%20-%20Pattern%20Recognition%20And%20Machine%20Learning%20-%20Springer%20%202006.pdf

Castells, M. (2009). Comunicación y Poder. Alianza Editorial.

Chesñevar, C. y Estevez, E. (2018). El comercio electrónico en la era de los bots. En *Algoritmolandia* (pp. 127-135). Planeta

Corvalán, G. (2018). Estados eficientes. En G. Beliz (Ed.), *Algoritmolandia (*pp. 257-263). Planeta.

Deleuze, G. (1999). *Conversaciones (1972-1990)*. Éditions de Minuit.

Galloway, S. (2018). Four*: El ADN secreto de Amazon, Apple, Facebook y Google*. Penguin Random House.

Galup, L. (2019). *Big Data & Política: de los relatos a los datos. Persuadir en la era de las redes sociales*. Penguin Random House.

Han, B. (2017). *La expulsión de lo distinto*. Herder Editorial.

Han, B. (2013). *La sociedad de la transparencia*. Herder Editorial.

Lannquist, Y. y Miailhe, N. (2018). Un desafío de gobernanza mundial. En G. Beliz (Ed.), *Algoritmolandia* (pp. 2019-231). Planeta.

Laswell, H. (1927). *Teoría política de la propaganda*. The American Political Science Review.

Lavista, J. (2018). El riesgo moral en el aprendizaje automático. En G. Beliz (Ed.), *Algoritmolandia* (pp. 245-252). Planeta.

Levy Daniel, M. (2016). *Servicios Over-the-Top: principios fundamentales para su tratamiento regulatorio en Argentina*. CELE.

Lessig, L. (1998). *Las leyes del ciberespacio*. Conferencia Taiwan Net '98. MIMEO.

Magnani, E. (2014) *Tensión en la red: Libertad y control en la era digital*. Autoria Sherpa.

Marr, B. (2016). *Big Data en Práctica: Cómo 45 empresas exitosas usaron Analítica de datos para encontrar resultados extraordinarios*. Wiley.

Mayer, V. y Cukier, K. (2013). *Big Data. La Revolución de los datos masivos*. Turner.

Murphy, K. (2013). *Machine Learning*. Cambridge. https://www.cs.ubc.ca/~murphyk/MLbook/pml-intro-22may12.pdf

O'Neal, C. (2016). *Armas de destrucción matemática. Cómo el Big data aumenta la desigualdad y amenaza la democracia*. Broadway Books.

Pariser, E. (2017). *El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamos*. Taurus.

Peirano, M. (2018). *El enemigo conoce el sistema*. Debate.

Rao, A. (2018). Una nueva etapa de globalización. G. Beliz (Ed.), *Algoritmolandia* (pp. 51-60). Planeta.

Roseth, B. (2019). *El fin del trámite eterno*. Banco Interamericano de Desarrollo.

Siri, J. y Serur, J. (2018). Trading Algoritmico. En *Algoritmolandia* (pp. 205-215). Planeta.

Srnicek, N. (2018) *Capitalismo de plataformas*. Caja Negra Editora.

Sosa Escudero, W. (2019). *Big Data: breve manual para conocer la ciencia de los datos que ya invadió nuestras vidas*. Siglo XXI.

Varian, H. y Shapiro, C. (1998). *La economía de la información*. Harvard Business School Press.

Winner, L. (2008*). La ballena y el reactor: una búsqueda de los límites en la era de la alta tecnología*. Gedisa.

Recursos Electrónicos

Alvarez, R. (20 de junio de 2018). “El reconocimiento facial se sigue expandiendo en China: los metros de Beijing y Shanghai incorporarán sistemas biométricos”. En X*akata.* Recuperado de https://www.xataka.com/privacidad/reconocimiento-facial-se-sigue-expandiendo-china-metro-beijing-shanghai-incorporan-sistemas-rastreo-biometrico

(29 de julio de 2020). “Amazon es cuestionado por explotar datos de terceros y por buscar vencer a competidores más pequeños”. En El ceo. Recuperado de https://elceo.com/tecnologia/amazon-comparecencia-jeff-bezos-congreso/

Arana, I. (18 de mayo de 2019). “La inquietante apuesta china por el reconocimiento facial”. En *La Vanguardia.* Recuperado de https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html

(1 de agosto de 2020). "Australia hará que Facebook y Google paguen por el contenido de los medios". En *El Tribuno.* Recuperado de https://www.eltribuno.com/jujuy/nota/2020-8-1-11-31-0-australia-hara-que-facebook-y-google-paguen-por-el-contenido-de-los-medios

Berchi, M. (12 de febrero de 2020). "¿Qué hace Facebook con los datos de las personas?". En *Ámbito.* Recuperado de https://www.ambito.com/informacion-general/facebook/que-hace-los-datos-las-personas-n5082358

Balbi, M. (25 de noviembre de 2017). "Los 7 secretos del país más digital del mundo". En *Infobae.* Recuperado de https://www.infobae.com/tendencias/innovacion/2017/11/25/los-7-secretos-del-pais-mas-digital-del-mundo/

Becerra, M. "Tus zonas erróneas". En *Anfibia.* Recuperado de http://revistaanfibia.com/ensayo/tus-zonas-erroneas/

Berchi, M. (19 de diciembre de 2019). "La gente no tiene conciencia de lo que hace cuando usa el celular". En *Ámbito.* Recuperado de https://www.ambito.com/negocios/app/la-gente-no-tiene-conciencia-lo-que-hace-cuando-usa-el-celular-n5072138

Berchi, M. (22 de octubre de 2019). “Prometea, inteligencia artificial para hacer Justicia”. En *La Nación.* Recuperado de https://www.ambito.com/politica/justicia/prometea-inteligencia-artificial-hacer-n5061091

Cadwalladr, C. (18 de marzo de 2018). “”Yo diseñé el arma de guerra psicológica de Steve Bannon”: conozca al denunciante de esta guerra de datos”. En *The Guardian.* Recuperado de https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

Candel, J., Prat, M. (28 de marzo de 2019). “Google Adsense: multa de 1.490M€ por abuso de dominio en publicidad en línea”. En *Blog Cuatrecasas.* Recuperado de https://blog.cuatrecasas.com/competencia/google-adsense-multa-1490-abuso-dominio-publicidad-linea/#:~:text=Google%20AdSense%3A%20Multa%20de%201.490,dominio%20en%20publicidad%20en%20l%C3%ADnea&text=AdSense%20for%20Search%20funciona%20como,propietarios%20de%20sitios%20web%20editores.

(4 de octubre de 2019). “Cámaras de reconocimiento facial: Larreta prometió 10.000 más”. En *Página 12.* Recuperado de https://www.paginoa12.cm.ar/223372-camaras-de-reconocimiento-facial-larreta-prometio-10-000-mas

(24 de julio de 2019). "Cambridge Analytica: la multa récord que deberá pagar Facebook poor la forma que manejó los datos de 87 millones de usuarios". En *BBC.* Recuperado de https://www.bbc.com/mundo/noticias-49093124

Castells, M. (2003). Internet, libertad y sociedad: una perspectiva analítica. *POLIS, Revista Latinoamericana*. https://www.redalyc.org/articulo.oa?id=305/30500410

(27 de junio de 2017). "China endurece su ley de protección de datos". En *Equipo PSN Sercon.* Recuperado de https://blog.psnsercon.com/china-endurece-su-ley-de-proteccion-de-datos/

(1 de octubre de 2019). “China presentó una super cámara de 500 megapíxeles para reconocimiento facial en multitudes”. En *La Nación.* Recuperado de https://www.lanacion.com.ar/tecnologia/china-presento-super-camara-500-megapixeles-recon ocimiento-nid2292766

(30 de julio de 2020). "El fundador de Instagram tuvo miedo de Facebook y ésa puede ser la prueba que condene a Zuckerberg". En *Yahoo Finanzas.* Recuperado de https://es-us.finanzas.yahoo.com/noticias/fundador-instagram-miedo-facebook-122002235.html

Diez, P. (20 de mayo de 2019). "El «Gran Hermano» chino lo ve todo con cámaras que reconocen caras en segundos". En *ABC.* Recuperado de https://www.abc.es/sociedad/abci-gran-hermano-chino-todo-camaras-reconocen-caras-segundos-201905190159_noticia.html

(27 de julio de 2018). "El reconocimiento facil de Amazon confunde a 28 congresistas con sospechosos de la policía". En *El País.* Recuperado de https://elpais.com/tecnologia/2018/07/27/actualidad/1532683160_968681.html

Ferreyra, E. (2017) "Desafíos de la biometría para la protección de los datos personales – Reflexiones sobre el caso SIBIOS". En *ADC (Asociación por los Derechos Civiles).* Recuperado de

https://adc.org.ar/wp-content/uploads/2019/06/030-desafios-de-la-biometria-para-la-proteccion-de-datos-05-2017.pdf

Freedom of Expression and the Internet in China. A Human Rights Watch Backgrounder. Recuperado de https://www.hrw.org/legacy/backgrounder/asia/china-bck-0701.html

Goldfarb, A. y Trefler, D. (2017). *IA y Comercio Internacional*. NBER y Universidad de Toronto. http://www-2.rotman.utoronto.ca/~dtrefler/papers/Goldfarb_Trefler_AI_2017.pdf

(10 de octubre de 2018). "Google apela una multa récord de USD 4.991 millones por Android. En *Infobae.* Recuperado de https://www.infobae.com/america/tecno/2018/10/10/google-apela-multa-record-de-usd-4-991-millones-de-ue-por-android/

Gonzalez, Fernanda (31 de julio de 2020). "Amazon confirma lo que ya sabíamos: Utilizó los datos de sus clientes para optimizar marcas propias". En *Merca2.0*. Recuperado de https://www.merca20.com/amazon-confirma-lo-que-ya-sabiamos-utilizo-los-datos-de-sus-clientes-para-optimizar-marcas-propias/

Guida, M., Himelfarb, G. y Sanchez Porto, M. (2009). *Protección de Datos Personales en la Sociedad Del Conocimiento: El polémico caso del Decreto 625/09*. MIMEO.https://www.dropbox.com/sh/xws6rmuxj036uuf/AAB-

J0aoA1CzK6X8EzVnO3O0a?dl=0&preview=GUIDA%2C+M.+Clara%3B+HIMELFARB%2C+Gonzalo%3B+SANCHEZ+PORTO%2C+Monserrat+-+Protecci%C3%B3n+de+los+datos+personales+en+la+Sociedad+del+Conocimiento+el+pol%C3%A9mico+caso+del+Decreto+625-09.pdf

Hayon, Alejandra (3 de agosto 2019). "Seis días arrestado por un error del sistema de reconocimiento facial". En *Página12.* Recuperado de https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

Hughes, Chris (9 de mayo de 2019). "Es hora de desarmar a Facebook". En *Infobae.* Recuperado de https://www.infobae.com/america/the-new-york-times/2019/05/09/es-hora-de-desarmar-a-facebook/?fbclid=IwAR0AtjI-ycXig9Ei-iaY8H8MfNeMnUyI70lVV-Iikj6FtYcQcclt7OvAIRw

"Internet de las Cosas". Informe del Ministerio de Modernización. Disponible en: https://www.argentina.gob.ar/sites/default/files/paperbenchmarkinternacional-iot.pdf

Investigación de la competencia en los mercados digitales. Subcomité Antimonopolio del Comité Judicial de la Cámara de Representantes EEUU. Octubre 2020.

Jaimovich, D. (20 de noviembre de 2019). "Cómo Estonia se convirtió en el país más digital del mundo". En *Infobae*. Recuperado de https://www.infobae.com/tecno/2019/11/20/como-estonia-se-convirtio-en-el-pais-mas-digital-del-mundo/

Kaufman, E. (2005). "E-Democracia local en la gestión cotidiana de los servicios públicos: modelo asociativo (Público-Privado) de gobierno electrónico local". En S. Finkelevich (coord.), *E-Política y E-Gobierno en América Latina*. https://www.dropbox.com/sh/xws6rmuxj036uuf/AAB-J0aoA1CzK6X8EzVnO3O0a?dl=0&preview=KAUFMAN%2C+Ester+(2005).+%E2%80%9CE-Democracia+local+en+la+gesti%C3%B3n+(...).pdf

(2019) "Las empresas se han rezagado en el cumplimiento de GDPR: a más de un año de su implementación, sólo 28% cumplen." En *Capgemini.* Recuperado de

https://www.capgemini.com/mx-es/wp-content/uploads/sites/24/2019/09/Las-empresas-se-han-rezagado-en-el-cumplimiento-de-GDPR.pdf

Laufer, D. (2009). *Apuntes sobre e-gobierno en la Argentina. Definiciones del concepto, historia del decreto y pautas de análisis para tomar en cuenta en los trabajos*. MIMEO. https://www.dropbox.com/sh/xws6rmuxj036uuf/AAB-J0aoA1CzK6X8EzVnO3O0a?dl=0&preview=LAUFER%2C+Dar%C3%ADo+(2009).+Apuntes+sobre+e+gobierno..pdf

Lee, Timothy B. (30 de Julio de 2020). “Emails detail Amazon’s plan to crush a startup rival with price cuts”. En *Arstechnica*. Recuperado de https://arstechnica.com/tech-policy/2020/07/emails-detail-amazons-plan-to-crush-a-startup-rival-with-price-cuts/?comments=1

Ley Nº 25.326/2000 de Protección de Datos Personales. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Lowry, S., Macpherson, G. (1988). *Una mancha en la profesión*. British Medical Journal.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2545288/pdf/bmj00275-0003.pdf

Lukyanov, D. (23 de mayo de 2019). “El Gran Hermano te vigila: el impenetrable Escudo Dorado de China que 'protege' su internet de EEUU”. En *Sputnik.* Recuperado de https://mundo.sputniknews.com/asia/201905231087364992-escudo-dorado-de-china-protege-su-internet-de-eeuu/

McCarthy, J. (2007). "¿Qué es la Inteligencia Artificial?". En *Formal Standord.* Recuperado de http://www-formal.stanford.edu/jmc/whatisai/node1.html

Mcloughiln, M. (29 de julio de 2020). "¿Es la App Store un monopolio? El plan de Apple para evitar otra multa millonaria?". En *El Confidencial.* Recuperado de https://www.elconfidencial.com/tecnologia/2020-07-29/app-store-competencia-acusaciones-monopolio_2698184/

(19 de mayo de 2020). "Multan en la Argentina a Google por no permitirle a una usuaria acceder a sus datos personales". En *Télam.* Recuperado de: https://www.telam.com.ar/notas/202005/465522-multan-en-la-argentina-a-google-por-no-permitir-a-una-usuaria-acceder-a-sus-datos-personales.html

Parra, S. (5 de octubre de 2019). “En China se tendrá que hacer un reconocimiento facial a todo aquel que solicite un número de teléfono”. En *Xakata.* Recuperado de

https://www.xatakaciencia.com/tecnologia/china-se-tendra-que-hacer-reconocimiento-facial-a-todo-aquel-que-solicite-numero-telefono

Pascual, M. (20 de agosto de 2019). "Visión y tecnología Maimunah Mohd Sharif: "Ciudad Inteligente no implica tecnología de punta"". En *Revista Retina.* Recuperado de https://retina.elpais.com/retina/2019/08/19/talento/1566221330_923849.html

Pecharromán, X. (28 de septiembre de 2019). “Las grandes empresas españolas, entre las más atrasadas en protección de datos”. En *elEconomista*. Recuperado de https://www.eleconomista.es/economia/noticias/10109134/09/19/Las-grandes-empresas-espanolas-entre-las-mas-atrasadas-en-proteccion-de-datos.html

Pehlivan, C. (1 de julio de 2020). “RGPD: balance de dos años y una aplicación no tan armonizada en la UE”. En *elEconomista*. Recuperado de https://www.eleconomista.es/opinion-blogs/noticias/10639960/07/20/RGPD-balance-de-dos-anos-y-una-aplicacion-no-tan-armonizada-en-la-UE.html

Plummer, L. (22 de agosto de 2017). “Así es como funciona el sistema ultra secreto de recomendación de Netflix”. En *Wired.* Recuperado de https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like

Poza Martín, R (11 de junio de 2020). "Amazon se enfrenta a acusaciones de monopolio por parte de la UE". En *Finanzas.com.* Recuperado de https://www.finanzas.com/empresas-globales/amazon-se-enfrenta-a-acusaciones-de-monopolio-por-parte-de-la-ue_20071596_102.html?fbclid=IwAR0-17Ofr5MBX9Pm0W7qdpxGegJDWciCxXohEvwG-8AB4CTHnR6hfiAAhCc

Prince, A. (2002). *Gobierno digital en la Argentina, Un breve white paper.* https://www.dropbox.com/sh/xws6rmuxj036uuf/AAB-J0aoA1CzK6X8EzVnO3O0a?dl=0&preview=PRINCE%2C+Alejandro+(2002).+Gobierno+digital+en+la+Argentina.+Un+breve+white+paper..pdf

Raffath, H. (2016). “Los chatbots son el futuro. 80% de las compañías quieren integrarlos para el año 2020”. En DazeInfo. https://dazeinfo.com/2016/12/15/chatbot-market-potential-adoption-2020-report/

Reglamento General de Protección de Datos Personales (UE) 2016/679. Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf y https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Rivera, N. (12 de febrero de 2017) “Usando internet en China durante una semana: una pradera repleta de vallas”. En *Hipertextual.* Recuperado de https://hipertextual.com/2017/02/internet-china

Sábato, J. y Botana, N. (1993). *La ciencia y la tecnología en el desarrollo futuro de América Latina*. http://docs.politicascti.net/documents/Teoricos/Sabato_Botana.pdf

Sampietro, N. y Costa, M. (2018). Cuando el gobierno innova. En G. Beliz (Ed.), *Algoritmolandia* (pp. 266-269). Planeta.

(15 de mayo de 2019). “San Francisco prohíbe el sistema de reconocimiento facial”. En *Página 12.* Recuperado de https://www.pagina12.com.ar/193938-san-francisco-prohibe-el-sistema-de-reconocimiento-facial

(15 de mayo de 2019). "San Francisco prohíbe el uso de reconocimiento facial para identificar criminales. En *La Vanguardia.* Recuperado de https://www.lavanguardia.com/internacional/20190515/462256381193/san-francisco-reconocimiento-facial-prohibe.html

Scholz, M., Dorner, V., Schryen, G. (2017). Configuraciones basadas en sistemas de recomendación para soporte y decisiones de e-commerce. https://www.researchgate.net/publication/308722432_A_configuration-based_recommender_system_for_supporting_e-commerce_decisions

Scrollini, F. (2019). “Automatizar con cautela. Datos e Inteligencia Artificial en América Latina.” En *ILDA (Iniciativa Latinoamericada por los Datos Abiertos).* Recuperado de

https://idatosabiertos.org/automatizar-con-cautela-datos-e-inteligencia-artificial-en-america-latina/

Smith, B. y Linden, G. (2018*). Dos décadas de sistemas de recomendación en Amazon.com*. IEEE Internet Computing. https://assets.amazon.science/76/9e/7eac89c14a838746e91dde0a5e9f/two-decades-of-recommender-systems-at-amazon.pdf

Snow, Jacob. (2018). "El sistema de reconocimiento facial de Amazon confudió a 28 miembros del congreso con sospechosos buscados por la policía". En *ACLU (Unión Estadounidense por las Libertades Civiles).* Recuperado de https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Velázquez, M. (2004). *La Necesidad de regular el uso de las Nuevas Tecnologías*.

Wu J y Lam W. (5 de septiembre de 2017).“Evolución del Gran Cortafuegos chino: 21 años de censura”. En *Global Voices.* Recuperado de https://es.globalvoices.org/2017/09/05/evolucion-del-gran-cortafuegos-chino-21-anos-de-censura/