Jorge Litvin* y Cecilia Danesi**

* Abogado por la Universidad de la Cuenca del Plata (UCP), especialista y maestrando en derecho penal por la Universidad Torcuato Di Tella (UTDT), especialista en Cibercrimen y evidencia digital por la Universidad de Buenos Aires (UBA) y diplomado en Litigación Oral Penal por la American University Washington College of Law (AUWCL). Además, completó el posgrado Iberoamericano en Cibercrimen e investigaciones digitales por la Universidad de Hartman y el Programa en Derecho de Internet y Tecnología de las Comunicaciones de la Universidad de San Andrés (UDESA). También realizó cursos de posgrado en las Universidades de Harvard, Yale y del Estado de Nueva York. Se desempeña como litigante en el Estudio Nercellas y es Chief Legal Officer (Director de legales) en Resguarda, a su vez es consultor integrante del Laboratorio de Ciberseguridad de la OEA (Organización Estados Americanos). Es autor del libro *Hackeados. Delitos en el mundo 2.0 y medidas para protegernos.*

** Abogada por la Universidad de Buenos Aires (UBA). Magister en Derecho de Daños, Universidad de Girona (España) con beca de la Fundación Carolina (tesina en IA y responsabilidad civil). Estudió en las Universidades de Salamanca y Paris 2-Panthéon. Investigadora y docente de la UBA. Directora de la revista *Inteligencia Artificial, Tecnologías Emergentes y Derecho* (Hammurabi). Doctoranda del Doctorado internacional en Derecho del Consumidor de las Universidades de Perugia y Salamanca. Correo: ccdanesi@gmail.com IG @ceciliadanesi y LK: Cecilia Celeste Danesi.

Navaja suiza intelectual

Herramientas de inteligencia artificial para la prevención e investigación criminal[1]

Hoy truena la tormenta que ayer pronosticábamos para mañana. Llueven avances que nos inundan de nuevas tecnologías con las que convivimos, incluso sin saber de qué se tratan. Este diluvio forma parte de un punto de inflexión en la historia, un momento bisagra.

Mucho se ha escrito y hablado sobre esta "Cuarta Revolución Industrial", cuya protagonista es la inteligencia artificial (en adelante, también IA). La encontramos prácticamente en todos lados, aunque no siempre nos damos cuenta de que está, desde apps de entretenimiento que adecuan sus recomendaciones a nuestras preferencias, buscadores de Internet que se adelantan a lo que nos interesa, hasta vehículos que sin intervención humana se mueven por nuestras ciudades y, en lo que aquí interesa, en una navaja suiza llena de herramientas que pueden utilizar los Estados para frenar o dar una respuesta a la delincuencia.

En las siguientes páginas intentaremos –de la manera más sencilla posible– dar una noción básica de qué es la inteligencia artificial, para luego exponer los distintos sistemas basados en ella que actualmente asisten en la prevención e investigación de una cuestión criminal. Finalmente haremos unas breves reflexiones que pretenden dar lugar a nuevos debates.

II. En búsqueda de una definición de la IA

Es muy probable que lo primero que se nos venga a la mente cuando se menciona a la inteligencia artificial sea la imagen de robots todopoderosos dominando un futuro apocalíptico.

Apartémonos de Hollywood por un momento y tratemos de conceptualizar qué es la IA en la realidad -y en su nivel de desarrollo actual-. Abusando de su propia textualidad, pensemos a este fenómeno como la intención de dotar a las máquinas (creaciones del ser humano, no de la naturaleza) de "inteligencia", una cualidad que hasta el momento estaba reservada

1 Artículo presentado el 18 de noviembre de 2020.

exclusivamente a la humanidad. Más que dar un concepto procuraremos que se comprenda su funcionamiento.

Partamos de la base de que la "inteligencia" se encuentra en un *software* (igual que el de los celulares o computadoras), un programa compuesto por un gran conjunto de datos que pueden provenir de sensores (por ejemplo, sonidos captados por un micrófono o las imágenes tomadas por una cámara) y/o de un humano que los carga. Ese *data set* será el *input*, es decir los datos de entrada en el que se basarán las tareas y procesos de la máquina.

El siguiente paso es poner la máquina a "pensar". ¿Cómo lo hace? Todos los datos que capta serán procesados por un *algoritmo*. ¿Un algo… qué? Un algoritmo es una fórmula matemática compleja; una secuencia de pasos que la máquina sigue para lograr su objetivo. Para graficarlo podemos hacer un paralelismo con una receta de cocina; utilicemos de ejemplo una muy sencilla: mantequilla de maní. Una vez que contamos con los ingredientes (solo maní), sabemos que debemos 1) colocarlo en una procesadora de alimentos, 2) encenderla a máxima potencia y 3) aguardar con paciencia. Como consecuencia de haber respetado esos pasos obtendremos lo que deseamos, del mismo modo la máquina que respeta el algoritmo genera aquello para lo que la configuramos: una predicción o una acción que es conocida como *output*.

Recapitulando, el resultado "inteligente" se produce por aplicar un procedimiento a los datos con los que se programó el sistema y a los que la IA percibe del entorno en el que se encuentra (esto quiere decir que "aprende" del humano y, en parte, por sí misma). El nivel de autonomía de esas resoluciones tomadas por la tecnología es una de las cuestiones más debatidas hoy en día.

Concebimos ese bosquejo de explicación para que se comprenda de modo sencillo. Para un concepto más detallado y técnico podemos remitirnos al del Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial de la Unión Europea: "Los sistemas de inteligencia artificial (IA) son sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores" (del documento *Una definición de la inteligencia artificial: principales capacidades y disciplinas científicas*)[2].

No podemos perder de vista que solo con indagar en las dificultades que existen en torno a conceptualizar qué es la *inteligencia* por sí sola podemos imaginar lo que nos depara tratar de definir a la inteligencia artificial. De hecho, en un reciente documento del Parlamento Europeo se incluyeron nada menos que doce definiciones de diversos países[3], diccionarios y organismos internacionales sobre qué es la IA; una tecnología tan disruptiva que ni en su definición podemos consensuar.

En lo que sí hay consenso es en que la IA es una disciplina de estudio que tiene distintos campos, el más conocido -y en el que se basan la mayoría de las herramientas a las que nos

2 Accesible en: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top al 15/11/20.

3 European Parliament. (Julio de 2020). *Study: Artificial Intelligence and Civil Liability* - Legal Affairs. Disponible en https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf

vamos a referir de ahora en más- es el *Machine Learning* (aprendizaje de máquina) y, dentro de éste, un subcampo denominado *Deep Leaning* (aprendizaje profundo).

Esta investigación no pretende profundizar en esos conceptos ni en sus características técnicas. Solo procuramos que se comprenda de qué hablamos cuando hacemos alusión a este tipo de inteligencia. Pero antes de adentrarnos en lo que nos convoca repasemos respondiendo ¿qué hace la IA?: 1) obtiene datos que serán considerados para tomar decisiones, 2) "decide" qué acción se llevará a cabo, es decir, "predice" un resultado, y 3) "adapta" sus decisiones y conductas en base al entorno y al contexto. Procedamos ahora a ver qué nos permiten estos sistemas a la hora de prevenir, investigar y resolver sobre conductas delictivas.

II. Herramientas para prevenir el crimen

Si le proponemos que imagine herramientas que utilizan los policías para prevenir el crimen, ¿en qué pensaría? Probablemente en vehículos con sirenas y armas disuasivas. La respuesta no es desatinada, pero sí un tanto "vintage". El arma más efectiva serán las matemáticas y su vehículo las herramientas predictivas… o eso prometen las compañías.

II. 1. ¿Qué, dónde y cómo sucederá? *Minority report*, de la ficción a la realidad.

La policía cumple un rol trascendental en la sociedad que no se reduce a reaccionar ante la actividad criminal, sino más bien a evitar que ocurra. Para ello, a lo largo de la historia, las autoridades han implementado distintos modelos para adelantarse a la comisión de ilícitos en el afán de prevenirlos. Desde buscar apoyo en los comentarios de los propios ciudadanos[4] a basar sus operaciones en el estudio constante de estadísticas del pasado[5].

Como mencionamos, nos encontramos ante una nueva revolución industrial y digital que está transformando y renovando a casi toda actividad, incluyendo a la policial. De hecho, las autoridades fueron pioneras en delegar tareas que dependían de la capacidad del ser humano a herramientas que procesan enormes bases de datos. CrimeScan, RTMDx,Palantir, Patternizer y el resonante Predpol son algunos de los muchos programas que prometen pronosticar la ocurrencia de delitos en base a otros que ya ocurrieron[6].

Su función principal -aunque no la única- es "predecir" dónde y cuándo sucederán determinados ilícitos, de modo que las fuerzas policiales puedan coordinar estratégicamente el patrullaje de sus oficiales en las calles, asignando la cantidad de tiempo que deben recorren cada área y monitoreando aquellas que estén siendo sub o incluso sobre vigiladas[7].

4 En el siglo XIX las fuerzas de la ley implementaban el modelo de policía comunitaria (*community policing*) que se basaba en la colaboración y consulta constante a los ciudadanos, cuya voz se consideraba determinante para prevenir e investigar actividades criminales. Ver Skogan Wesley G. (2006). The Promise of Community Policing. En *Police Innovation. Contrasting Pcrspectives*. Cambridge Studies in Criminology. Cambridge University Press, Nueva York. Págs. 27-43.

5 En 1994, el departamento policial de la ciudad de Nueva York empezó a implementar CompStat, un sistema de rendición de cuentas del desempeño de las autoridades que mutó en una herramienta de organización policial basada en la aplicación de inteligencia y análisis de datos estadísticos de crímenes pasados. Puede considerarse un precedente de los sistemas actuales de IA que se analizaran. Hoy, el sistema sigue vigente en su update CompStat 2.0, que da acceso al público de las estadísticas de los delitos. Ver https://www1.nyc.gov/site/nypd/stats/crime-statistics/citywide-crime-stats.page

6 Debemos aclarar que estas herramientas también fueron concebidas para predecir otros hechos no delictivos como eventos médicos y accidentes viales, y se comercializan a empresas y organizaciones del sector privado además de las fuerzas públicas policiales. Por la finalidad y extensión de este artículo, esas aplicaciones no serán sujetas a nuestro análisis.

7 El funcionamiento de la herramienta se puede ver en PredPol & Open Goverment Data – PredPol – YouTube. Accesible mediante el siguiente enlace https://youtu.be/b6PWiisfIy4.

¿Cómo funcionan? La policía vuelca en el software los datos de los delitos que se cometieron en su jurisdicción en los últimos años, en el caso de Predpol se cargan solo tres: 1) tipo de ilícito (por ejemplo: robo, utilización de armas de fuego), 2) ubicación del evento, y 3) momento -fecha y hora exactos- en el que ocurrió. Luego la "inteligencia" se sigue entrenando de forma continua mediante la carga de datos de nuevos delitos que se vayan registrando día a día, así se actualizan las zonas de patrullaje a medida que mutan las tendencias delictivas.

El programa resalta "zonas de calor" que representan cuán probable es que ocurra un delito en una zona determinada del mapa de la ciudad[8]. Además, dibuja cuadros de color rojo que representan micro-zonas[9] de mayor riesgo para cada día y para el turno correspondiente (diurno - tarde - nocturno), en donde se detallan los eventos más habituales en el área marcada. En base a las predicciones obtenidas, los policías son instruidos para dedicarle un porcentaje del tiempo de patrullaje a esas zonas de riesgo[10].

En otras palabras, la aplicación de la IA se resume en analizar los datos de delitos que ya sucedieron y establecer en el mapa la probabilidad de que vuelvan a ocurrir en determinada área y zona horaria. La lógica es que los policías patrullando esas zonas consideradas especialmente peligrosas pueden disuadir de que se cometan ilícitos o intervenir en el mismo momento delictivo[11].

El éxito de Predpol (de ventas al menos) llevó a que otras compañías también desarrollen herramientas similares añadiendo rasgos particulares. Por ejemplo, RTM (Risk Terrain Modeling) agrega a la ecuación otros datos relacionados con el entorno (si el lugar está cerca de un acceso al subterráneo y hasta el pronóstico climático). SSPSS de IBM (Statistical Package for the Social Sciences) toma en consideración que determinados crímenes son más probables en fechas específicas, por ejemplo: hurtos en la calle en los días de pago de salarios, irrupción a residencias en vacaciones cuando muchas familias están de viaje, etc.[12]. Mientras que HunchLab agrega a todo lo referido la consideración de la densidad poblacional, comercios o lugares que hay en zonas puntuales (bares, restaurantes, hospitales, paradas de transporte público), datos geográficos detallados (elevación, tipo de terreno, cercanía con cuerpos de agua natural) y de horarios en contexto (no solo se considera la hora puntual, sino también si ella coincide con el horario de la jornada escolar o laboral para calcular la probabilidad de determinada actividad criminal)[13].

II. 2. Hacia una policía robotizada

¿Le suena el nombre Alex Murphy? Quizás lo recuerde más como el protagonista de la ficción Robocop, un oficial fallecido que fue "resucitado" como un *ciborg* (mitad robot, mitad humano). En su último remake pudimos ver lo que probablemente apreciemos en las fuerzas policiales en unos años: humanos equipados con IA, sistemas de reconocimiento facial, GPS incorporado y la capacidad para

8 Se resaltan en verde, amarillo y rojo según va aumentando el índice de probabilidad.

9 Las micro-zonas se circunscriben a áreas de 150 metros cuadrados.

10 La cantidad de tiempo que debe dedicarse a cada zona es establecida por las autoridades, el software solo señala aquellas que estima más riesgosas. La mayoría de los departamentos policiales que lo implementaron instruye a sus oficiales para que pasen al menos el 10% de su turno patrullando las áreas marcadas por PredPol.

11 Predpol se utiliza en muchos departamentos policiales de los Estados Unidos, a diferencia de las demás herramientas similares ya desembarcó en Latinoamérica. Lleva cinco años desde su implementación por la Jefatura de Policía de la Ciudad de Montevideo (Uruguay). Ver más en https://policia.minterior.gub.uy/index.php/noticias-y-comunicados-de-prensa/2320-predpol.

12 Por el momento, SSPSS fue implementado por la policía de Richmond, Edmonton, Durham, Memphis, Miami-Dade y Manchester.

13 Por el momento, HunchLab fue implementado por la policía de Nueva York (como piloto), Tacoma, Pierce Country, Ohio, St Lous, Peoria, Philadelphia, Lincoln y New Castle.

identificar riesgos mediante el procesamiento acelerado de bases de datos.

No nos dedicaremos a "predecir el futuro" en este trabajo. Entendemos más prudente y pragmático dedicar estas páginas a analizar las herramientas con las que ya contamos. Sin embargo, no podemos pasar por alto que la pandemia de la Covid-19 aceleró algunos pasos. Países como China y Emiratos Árabes ya equiparon a sus fuerzas policiales con "cascos inteligentes" que dotan a los oficiales de herramientas de escaneo masivo de temperatura corporal, de patentes de vehículos y reconocimiento facial (aun cuando los individuos lleven puesto un barbijo)[14].

Un poco más cerca en geografía, pero dando un paso más lejano en tecnología, la policía de California ya está utilizando robots completamente autónomos con Inteligencia Artificial que patrullan y monitorean espacios públicos[15]. Aun cuando no están armados y son inofensivos, se presentan como una herramienta eficaz de disuasión delictiva. Cuentan con cámaras de 360º equipadas con software de reconocimiento facial y lectura de patentes vinculadas a las bases de datos que incluyen a individuos sospechosos o buscados. Evidentemente el futuro que imaginábamos está mucho más cerca de lo que pensábamos.

III. Herramientas para prevenir e investigar el crimen

Una comunidad que instala pantallas y micrófonos que registran las conversaciones que los ciudadanos tienen en las calles y en sus casas, y una fuerza policial pendiente de esa información para prevenir y castigar crímenes. Podría pensarse que estamos describiendo lo que está pasando, pero eso forma parte de la trama de ficción publicada por George Orwell hace más de setenta años (Orwell, 1949). En este capítulo mencionaremos algunas prácticas estatales que se han renovado y potenciado gracias a la IA; veremos que el nivel de intrusismo que las autoridades pueden lograr pone a la distopía orwelliana en un plano muy semejante a la actualidad.

III.1. Indicios y pruebas en entornos virtuales. La utilización de IA para OSINT y Ciberpatrullaje

La digitalización de la sociedad devino en que mucho de lo que sucedía en el "mundo real" se haya trasladado a su homónimo digital. Internet está plagada de acciones de los usuarios que -consciente o inconscientemente- publican dando acceso libre e irrestricto al resto de los conectados, incluyendo al Estado. Nuestros posteos, tweets, imágenes y los contactos e interacciones que hacemos en nuestras redes sociales pueden servir como prueba para iniciar o profundizar investigaciones criminales. ¿Cómo? A través de OSINT (siglas para *Open Source Intelligence*), que no es otra cosa que aplicar técnicas de inteligencia para recopilar y relacionar los datos que se encuentran a disposición de todos en Internet.

Esa inteligencia es realmente compleja de hacer, para lo cual basta con que pensemos en la colosal cantidad de datos que se alojan en Internet, sumemos los que se agregan con cada segundo que transcurre y tenemos una masa informativa cuyo análisis íntegro demanda más tiempo del que disponemos de vida[16].

Reconociendo la dificultad análoga a buscar una aguja en un pajar, varias empresas desarrollaron herramientas de IA que mediante

14 *Coronavirus: Chinese police wear Smart helmets to check body temperature in crowds.* South China Morning Post. Disponible en https://youtu.be/WXULTL91Qwg.

15 *Police in California Unleash Their Own Robocop.* CBS Miami. Disponible en https://youtu.be/-REu3WQ789k

16 Para tener una noción de la cantidad de datos que hay en Internet recomendamos visitar https://www.internetlivestats.com.

sus algoritmos pueden encontrar, recopilar y comparar información, destacar la relevante en base a factores como nombres, geolocalización, *hashtags* o palabras clave, y elaborar informes preliminares que las autoridades pueden tomar como puntapié inicial en las investigaciones criminales. El rastrillaje de todo ese contenido -en los tiempos que demanda una investigación delictiva- solo es posible gracias a la capacidad de procesamiento y la algoritmización de la tecnología[17].

III. 2. Sonría, lo estamos filmando. Bienvenidos a "Gran Hermano"

Hace añares que se utilizan cámaras para prevenir e investigar delitos[18]. El primer objetivo se torna evidente en el momento en el que nos ponemos en los zapatos de un delincuente, que al advertir un dispositivo que lo registra es probable que desista de realizar la conducta delictiva. Si ese mismo sujeto no se percata o no es disuadido por la presencia del dispositivo, las imágenes tomadas servirán para identificar e investigar el hecho que no pudo ser prevenido.

Las ciudades están plagadas de estos dispositivos, ya ni siquiera nos resultan llamativos y hemos naturalizado que constantemente se tomen nuestros registros. Los organismos estatales los instalan en parques, puntos turísticos al aire libre, estaciones de transporte, aeropuertos y casi cualquier espacio público que imaginemos. Por su parte, las empresas y locales comerciales los colocan a la vista de todos y en puntos clave, mientras que muchísimas personas optan por un sistema de monitoreo para la seguridad de sus hogares.

Esa tecnología no escapó de la revolución algorítmica. Los sistemas ahora no solo transmiten y graban imágenes, sino que además pueden cruzarlas, compararlas y enlazarlas a un sinnúmero de datos gracias al *machine learning* aplicado a la *big data*. La clasificaremos en dos grandes grupos en base a los factores de reconocimiento de los que es capaz.

El primero está integrado por aquellas que pueden identificar patrones biométricos. Los circuitos de video tradicionales registran las acciones de las personas en un determinado lugar y momento, pero los nuevos sistemas además pueden reconocer instantáneamente la identidad del sujeto. ¿Cómo saben quién es quién? Mediante matemática aplicada a la biometría[19]. Basta con pensar en la mayoría de los teléfonos inteligentes que se desbloquean solo cuando el usuario registrado lo mira, es exactamente la misma tecnología.

¿Cómo funcionan? Las cámaras son los sensores del sistema que captan imágenes y las comparan con otras que toman de las bases de datos que lo nutren. ¿Con qué imágenes? Dependiendo del sistema, se alimentan de las que se obtienen al tramitar documentos oficiales (como pasaportes o licencias de conducir)[20] o inclusive las *selfies* que publicamos en redes sociales[21].

17 Son muchas las herramientas, como meros ejemplos y en el afán de que pueda profundizarse sobre su funcionamiento recomendamos ver https://www.recordedfuture.com/ y https://www.paliscope.com.

18 Técnicamente se conoce a la tecnología como circuito cerrado de televisión (CCTV). La nomenclatura responde a que las imágenes tomadas solo pueden ser vistas por un grupo determinado de personas.

19 En pocas palabras definimos a la biometría como patrones que nos hacen únicos distinguiéndonos del resto. Nuestra retina, las facciones de nuestro rostro y las huellas dactilares de nuestros dedos son ejemplos habituales.

20 Por ejemplo, en Argentina se implementó el Sistema de Reconocimiento Facial de Prófugos (SRFP) en la Ciudad de Buenos Aires con el fin de ubicar a las personas con pedido de captura. Gracias a la solicitud de información pública efectuada por la Asociación por los Derechos Civiles (ADC) se pudo conocer que la base de datos utilizada por el sistema es la de Consulta Nacional de Rebeldías y Capturas (CONARC) y los datos biométricos del Registro Nacional de las Personas (RENAPER). Ver https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires

21 Por ejemplo, el software Clearview AI es una herramienta que está siendo utilizado por las organizaciones policiales de muchos países, incluyendo a INTERPOL (dentro de Latinoamérica en Brasil) para la investigación de delitos. Su tecnología de *deep learning* promete identificar a los sospechosos y/o a las víctimas mediante un motor de búsqueda

En el segundo grupo incluimos todas las herramientas que permiten identificar patrones distintos a los biométricos. ¿Cuáles? La IA permite escanear y detectar masivamente la temperatura corporal de las personas[22], alertar de movimientos, patrones de conducta, símbolos o vestimentas que hayan sido configurados previamente como sospechosos[23], identificar patentes y marcas de vehículos o inclusive individualizar armas[24] u otros objetos sospechosos en espacios concurridos (por ejemplo, equipaje desatendido en aeropuertos o paquetes dejados en la vía pública)[25].

Cuando la IA detecta una correlación para la que fue entrenada (por ejemplo, si la cámara capta a una persona cuyos rasgos concuerdan con los de un sospechoso que está siendo buscado o la patente de un vehículo denunciado como robado) notifica en muy pocos segundos a las autoridades, de modo que puedan proceder a la persecución y eventual detención.

Lo descripto no es magia ni futurología: la IA es matemática avanzada implementada mediante tecnología. Esto quiere decir que el *output* obtenido siempre vendrá acompañado por una tasa de probabilidad de acierto (por ejemplo, el individuo A presenta una correlación biométrica con el individuo B del 80 %)[26], el sistema no es -y posiblemente nunca sea- perfecto, y aun cuando este trabajo pretende enfocarse en que se comprenda su funcionamiento, al final dejaremos planteados algunos cuestionamientos.

IV. Herramientas para investigar el crimen

A un paso acelerado se están desarrollando herramientas de IA que renuevan y potencian todos los procedimientos aplicables a una investigación criminal. Por la extensión propuesta no podemos abarcarlas a todas (además de que muchas probablemente no se implementarán), pero entendemos importante que conozcamos de su existencia y las perspectivas de evolución del proceso penal.

inversa de imágenes. El sistema se nutre de todas las bases de datos de fuentes abiertas incluyendo aquellas alojadas en redes sociales configuradas como públicas. Para más información ver https://clearview.ai y https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

22 En Argentina se instalaron cámaras térmicas en el Aeropuerto Internacional Ministro Pistarini y en algunas estaciones ferroviarias de la Ciudad de Buenos Aires. Ver https://www.argentina.gob.ar/noticias/el-gobierno-nacional-puso-en-marcha-las-camaras-termicas-en-el-aeropuerto-de-ezeiza y https://www.argentina.gob.ar/noticias/incorporamos-camaras-termicas-en-nuestras-estaciones , respectivamente.

23 Aunque no se aplica en Latinoamérica -o eso creemos-, no podemos dejar de comentar que en China se utiliza una herramienta muy poderosa basada en IA llamada CloudWalk que asegura -entre un enorme abanico de funciones- poder identificar los cambios bruscos o sospechosos en el comportamiento de los transeúntes. Por ejemplo, los movimientos de un "carterista" o de quien puede estar reconociendo el área para cometer un crimen en el futuro. La herramienta hace un seguimiento continuo del sospechoso luego de detectado el comportamiento. Ver https://www.cloudwalk.com/en/Technology.

24 El software ZeroEyes está siendo utilizado en varios colegios, universidades, aeropuertos y shoppings de los Estados Unidos y permite escanear masivamente a todos los que pasan por alguna de las múltiples cámaras de vigilancia que detectan si una persona porta un arma (ver más en https://zeroeyes.com). Lo mismo puede identificar Athena, un software muy potente que permitiría reconocer las armas aun cuando no estén a la vista gracias a un sensor térmico. Esta herramienta también pretende detectar peleas (dispara una alerta cuando el puño de una persona va a mayor velocidad de la configurada como habitual) o cualquier otra anomalía en el comportamiento de las personas, como cuando alguien se mueve mucho más lento o mucho más rápido que el resto de las personas a su alrededor. Puede verse más información al respecto en https://athena-security.com/ y https://www.defenseone.com/technology/2019/04/ai-enabled-cameras-detect-crime-it-occurs-will-soon-invade-physical-world/156502/

25 HikVision es uno de los softwares de IA aplicada a la videovigilancia con fuerte presencia en Latinoamérica, su funcionamiento es explicado someramente en https://www.hikvision.com/en/newsroom/latest-news/2018/technical-article---reducing-false-alarms-with-deep-learning/

26 Debe diferenciarse que la tecnología puede verificar la correlación biométrica entre dos personas u objetos determinados o bien, utilizarse para identificar a un sinnúmero de personas (quienes pasan por delante de la cámara) para contrastar sus facciones con todas las imágenes de las bases de datos recopiladas.

IV.1. Lobos disfrazados de corderos y bots disfrazados de indefensos

Desde 2013 hay una dulce niña filipina que constantemente busca interactuar con pedófilos y groomers en línea, se conecta a salas de chats y plataformas de citas. ¿Por qué se expondría y revictimizaría constantemente esa niña? Porque no existe, es un software que hasta hace poco era operado por agentes de la policía.

La pequeña "Sweetie"[27] se ve como una persona real a través de una webcam, y gracias a ella a miles de acosadores se pudieron detectar y enjuiciar, su última versión ya ni siquiera necesita de la operación de un humano para interactuar; se la dotó de inteligencia artificial y ahora cientos de *bots* están a la caza de todo depredador sexual que busque a sus víctimas en foros y plataformas de chat. Ese programa fue pionero en aplicar la tecnología conocida como CGI (Computer Generated Imagery) al proceso penal.

A principios de 2020 Samsung presentó el programa "Neon"[28], que son "avatares" de apariencia humana (escalofriantemente reales) dotados con IA avanzada que les permite autonomía en el aprendizaje. Aunque este proyecto no está pensado para procesos judiciales, nos permite ver un avance de lo que podemos esperar como asistentes autónomos en investigaciones criminales, parece no faltar mucho para generar "ejércitos" de agentes provocadores y/o encubiertos digitales.

IV.2. "Qué grandes orejas tienes IA…". Son para escucharte mejor.

Muchos sonidos pueden ser indicio de un delito; el del disparo de un arma de fuego es el ejemplo más nítido. Algunas armas pueden alcanzar una cadencia de hasta 900 proyectiles por minuto, en una fracción de ese tiempo la IA actual puede señalar el lugar dónde ocurrieron y exactamente qué arma los produjo. Shotspotter es el nombre de una de las herramientas que lo permite.

¿Cómo funciona? Está compuesta por sensores acústicos que se instalan en edificios y espacios públicos, que al detectar el sonido de un disparo estiman el lugar donde se produjo (en base al tiempo que le tomó a cada sensor captar el sonido) y el arma utilizada -aun cuando se utilizaran varias de forma simultánea- (los algoritmos consideran la nitidez, la fuerza y la duración de los sonidos, así como el tiempo de caída de los proyectiles). Esa información se envía al centro de monitoreo y automáticamente marca un punto rojo en los GPS que los oficiales utilizan en vehículos y celulares. Esto permite a las autoridades evitar que la situación escale, detener a los responsables o cuanto menos recuperar evidencia clave para la investigación[29].

IV. 3. No hay escape a la singularidad. Nuevas posibilidades de análisis de ADN mediante IA

Del abanico de medidas de prueba que se pueden realizar para identificar o vincular con un hecho a un criminal probablemente el análisis de ADN de las personas sea la evidencia estelar. Esto se debe a que cada uno es único e irrepetible, a pesar de ello las diferencias con el de otros individuos son muy sutiles (de un 0,1% aproximadamente[30]). A ese ínfimo

27 Para más información sobre "Sweetie" ver https://www.terredeshommes.nl/en/programs/sweetie.

28 Para más información acerca del proyecto "Neon" ver https://www.neon.life/.

29 El software también incluye herramientas "predictivas" como las analizadas previamente en este trabajo, generando planes de patrullaje en base a los datos con los que Shotspotter se va entrenando (ver punto II).
Para más información ingresar a https://www.shotspotter.com/technology/.

30 Así lo han determinado varios científicos, entre ellos podemos citar Mark Stockle y David Thalyer y su trabajo "*Why should mitocondria define species?*. Ver pág. 15. Accesible a través del siguiente enlace https://www.biorxiv.org/content/10.1101/276717v1.full.

margen hay que añadirle que las muestras obtenidas de la escena del crimen frecuentemente están incompletas o se componen de una mezcla de más de un ADN en simultáneo. Esas dificultades derivan en que se frustre la medida en muchos casos.

¿Cómo se determina a quién pertenece? Mediante la biomatemática, una conjunción de ciencias basada en cálculos complejos que demandan muchísimo tiempo y esfuerzo a un humano experto, procedimiento que es mucho más sencillo para las herramientas de IA que ya existen en este momento.

Programas de IA, como TrueAllele y STRmix, hacen análisis de genotipado probabilístico reconstruyendo muestras complejas o incompletas -como aquellos fragmentos que se obtienen de armas, dispositivos electrónicos, sorbetes, etc.-, separando los ADN de muestras mixtas e identificando correspondencia entre los rastros tomados y los cargados en bases de datos[31].

IV. 4. *Lie to me*

Seguramente podamos recordar al menos una serie o película con una escena en la que un sospechoso o un testigo declara conectado a un dispositivo que da indicios de si lo que dice es o no verídico. El polígrafo, también conocido como "detector de mentiras" no es una creación televisiva; es una herramienta que existe, aun cuando es muy cuestionada y de aplicación restrictiva. Ese instrumento se basa en la presión sanguínea, la frecuencia cardíaca y los cambios de polaridad en la piel de las personas para determinar si lo que dicen es verdad o mentira. Ese método ya devino "vintage".

Ahora las compañías están desarrollando y mejorando herramientas que detectarían mentiras reconociendo los mismos patrones que el Dr. Cal Lightman en la serie televisiva, pero de formas más… disruptivas. EyeDetect, por ejemplo, escanea la mirada del sujeto mientas es interrogado, el grado de dilatación de sus pupilas y el comportamiento de sus ojos lo califican como "veraz" o "engañoso" en tan solo unos minutos[32]. Silent Stalker va más allá, y hace un perfilamiento psicológico de las personas en base a marcadores no verbales de comportamiento analizados por algoritmos[33], tecnología que también dio nacimiento al cuestionado iBorderCtrl, un programa que se está testeando en Europa para controles migratorios basados -entre muchas cosas- en procedimientos algorítmicos de detección de mentiras.

V. Blandiendo una navaja de doble filo

Hasta aquí nuestro objetivo fue mostrar a la IA como una navaja suiza con un sinnúmero de herramientas de indudable utilidad para prevenir y/o investigar una acción criminal. Pero bien es sabido que las armas suelen tener dos filos, todo aquello que se presenta como un beneficio también acarrea riesgos y perjuicios.

No podemos pasar por alto que todos los sistemas que analizamos se convierten en productos luego de una gran inversión en investigación, esfuerzo y trabajo. ¿Por qué es importante? Porque significa que forman parte del mercado, ese campo de batalla en el que las compañías desarrolladoras compiten salvajemente por encontrar -y comercializar- la solución a un problema más rápido que sus adversarios.

31 Puede profundizarse sobre el funcionamiento de estas herramientas en https://www.cybgen.com y https://www.strmix.com.

32 EyeDetect es utilizado por organismos públicos y privados, puede accederse a más información en https://www.eyedetect.com.ua/en/eyedetect.html.

33 Para más información sobre Silent Talker acceder a https://www.silent-talker.com/.

El inconveniente que se presenta es que puede que las herramientas que den a luz en esta especie de "tecno guerra fría" entre privados no hayan pasado por todos los procesos de verificación y control de aspectos tan básicos como la eficacia y la seguridad, como consecuencia del apuro por ser las primeras en desembarcar en el mercado. Por su parte, los países también aspiran a ser los más innovadores y disruptivos en sus políticas de Estado, lo que hace que la ética o la legalidad de la utilización de estos programas pase a un segundo plano.

En este capítulo plantearemos algunas interrogantes que debemos responder antes de aclamar por la implementación de las herramientas que acabamos de ver.

V. 1 ¿Son fiables?

El concepto de fiabilidad remonta a la confianza que nos inspira algo o alguien. ¿Cuándo confiamos? Cuando podemos "relajarnos" de que aquello con lo que interactuamos (máquina o humano) cumplirá con su trabajo, funcionará debidamente o -cuanto menos- no va a producir un daño.

Tenemos una tendencia a confiar en las máquinas; se nos instaló la idea de que no fallan y siempre cumplen con aquello para lo que se las programa. Ese concepto mide una realidad fragmentada, olvida que su eficacia está condicionada por los componentes con que se arman y los datos que se les cargan, y que serán tan perfectas como los humanos por los que son creadas. Si algo ilustra claramente el concepto de utopía es la "perfección humana".

Cada uno de nosotros tiene parámetros propios para establecer un vínculo de confianza con otras personas y con las máquinas. Nos basamos en experiencias previas (no nos fiamos de quienes nos engañaron o lastimaron y tampoco en los productos que no funcionaron como esperábamos). Pero los efectos adversos que pueden producir las tecnologías que analizamos requieren que establezcamos algunos estándares mínimos antes de que puedan implementarse y salir al mercado. Los riesgos son muy elevados si esperamos a valorar la experiencia propia en cada caso. Si bien son varios los documentos que aspiran a establecer estándares mínimos de fiabilidad, tomaremos las Directrices Éticas de la Comisión Europea como guía para este trabajo[34], según las cuales la licitud, la ética y la robustez de los sistemas de IA son requisitos esenciales y necesarios. Intentemos desglosarlos.

V. 1. a) ¿Son lícitas?

Al momento de escribir este artículo no existe ni una legislación específica que regule las pautas para la creación, uso, ni mucho menos la responsabilidad por los daños que pueda ocasionar un sistema de IA. Para ello tenemos que acudir a las normas con las que ya contamos, las que -atendiendo al objeto de este trabajo- refieren a la Protección de Datos Personales, los Códigos Procesales Penales y los de fondo -tanto civiles como penales- para establecer eventualmente responsabilidades.

A pesar de que no estamos frente a un vacío regulatorio total, sí debemos considerar que el stock legislativo actual fue concebido para una sociedad en la que herramientas como las que estamos analizando solo existían en la ficción, pero no se contemplaban ni remotamente como una realidad. Veamos algunos supuestos para ejemplificar.

La Ley de Protección de Datos Personales de la Argentina ya tiene más de veinte años, ni siquiera existían *Facebook* o *Twitter* en aquella época, plataformas que son dos eslabones de una extensa cadena de bases de datos gigantescas que podemos encontrar en el entorno virtual, y que muchas compañías utilizan para nutrir sus herramientas de IA. Sin contar

34 Accesible en https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1.

con que ese tipo de leyes son las encargadas de determinar las pautas mínimas en materia de seguridad que todas las empresas deberían respetar[35].

La mayoría de los códigos procesales penales latinos -haciendo hincapié en el nacional argentino- se quedaron estancados en otro siglo. Sus normas fueron elaboradas para la obtención de evidencia física y -en muchos casos- para poder hacer uso de nuevas medidas investigativas se fuerza su interpretación con cuestionable analogía o se sobreexige a principios como el de "libertad probatoria" corriendo a ciegas por la cornisa de la vulneración a algunas garantías.

Ese último punto es fundamental, en tanto que no podemos desconocer la tendencia legislativa -al menos en Argentina- de generar parches normativos para dotar de legitimidad a métodos o instrumentos para los cuales existía un vacío legal. La activación del protocolo de implementación de ciberpatrullaje[36] a nivel nacional (recordando que ya se utilizaba sin legislar) o la aprobación de la tecnología de reconocimiento facial en la Ciudad de Buenos Aires son dos supuestos recientes que lo pueden ejemplificar[37].

No nos adentraremos en un análisis pormenorizado de la legislación argentina, ni mucho menos a la del resto de los Estados latinoamericanos, pero sí recordaremos que todos formamos parte del Sistema Interamericano de Derechos Humanos (entre otros tratados que ratificamos). No olvidemos que el contenido de su Convención tiene -al menos en Argentina- la más alta jerarquía legal. Eso quiere decir que cada normativa de nivel inferior que se pretenda incorporar en una legislación local debe respetar ineludiblemente a las garantías mínimas establecidas en ese texto convencional.

¿Qué derechos y garantías podrían afectar los sistemas que acabamos de analizar? Sin hacer futurología sino basándonos en circunstancias probadas (que ya fueron debatidas), podemos afirmar que las herramientas de policía predictiva y de reconocimiento facial tienen altas probabilidades de discriminar por motivos de raza, color, género, posición económica o condición social (en contradicción con lo dispuesto por los artículos 1.1 y 24 del Pacto de San José). Tampoco es difícil imaginar supuestos que pongan en jaque el derecho al debido proceso (artículo 8.1) y a la presunción de inocencia e igualdad (8.2).

En casos puntuales no podemos dejar de pensar en que la incapacidad de explicar y comprender cómo funcionan algunos de los sistemas aptos para generar evidencia en la que se funde una sentencia, presenta serios problemas a la hora de cuestionar e impugnar el resultado generado por la IA (artículo 8.2.h). Al respecto, la Comisión Europea ha señalado que las partes interesadas deben tener acceso y poder impugnar la validez científica de un algoritmo y la ponderación que se le dio a los diversos factores tenidos en cuenta.

Por su parte, la utilización indebida de herramientas de OSINT (para investigar o "ciberpatrullar") puede vulnerar el derecho a no ser objeto de injerencias arbitrarias en la vida privada (artículos 11.2 y 11.3) y poner en riesgo la libertad de expresión (artículo 13).

35 Vale mencionar al respecto que la Comisión Europea para la Eficiencia de la Justicia (CEPEJ) ha sostenido que las herramientas de IA deben desarrollarse y utilizarse contemplando los principios de protección de datos personales, y que todas las personas tienen derecho a no estar sujetas a decisiones que les afecten significativamente basadas únicamente en el procesamiento automatizado de datos.

36 Aunque luego se modificó el término por "prevención policial del delito con uso de fuentes abiertas". Ver Resolución 144/2020 -anexo I- del Ministerio de Seguridad, accesible en https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602.

37 Ver Ley 5688 del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires en http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley5688.html y la Resolución Nº 398/MJYSGC/19 accesible en https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf.

Debemos aclarar que los párrafos que preceden no implican una postura tendiente a obstaculizar la innovación en materia de prevención e investigación delictiva. Nuestra postura es más bien la contraria: celebramos el desarrollo e implementación de nuevas tecnologías, pero ello no puede venir escindido del avance en materia legislativa. Y para eso necesitamos una discusión profunda y genuina que contemple los efectos de esas herramientas y sus decisiones en los derechos de la ciudadanía.

V. 1. b) Reflexiones éticas a la implementación de IA

Partamos de la premisa aristotélica de que las acciones humanas son un instrumento para conseguir el bienestar (Aristóteles, 349 a.C.)[38], escenario en el cual la implementación de la IA debe perseguir la virtud, la mejora de las condiciones y calidad de vida para la humanidad.

En el sentido propuesto, pero mucho más cerca que el padre de la ética en el tiempo, el Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia en su documento *Directrices Éticas para una IA fiable* consideró que los sistemas de IA deben desarrollarse respetando la autonomía humana, previniendo la causación -o amplificación- de daños, garantizando la equidad, así como la transparencia y la explicabilidad de las decisiones tomadas por estas herramientas que nos pueden afectar.

En base a ello el documento insta a cumplir con las siguientes directrices: 1) acción y supervisión humanas, 2) solidez técnica y seguridad, 3) gestión de la privacidad y de los datos, 4) transparencia, 5) diversidad, no discriminación y equidad, 6) bienestar ambiental y social, y 7) rendición de cuentas.

Todo lo que acabamos de mencionar son miramientos que deben formularse durante todo el ciclo de vida de la inteligencia artificial. Desde que es concebida (se la idea, se deciden los datos a utilizarse, etc.), hasta que deja de estar en funcionamiento pues, al aprender permanentemente del entorno y recibir actualizaciones, los sistemas están en constante cambio y pueden dar respuestas discriminatorias luego de un tiempo de puestos en circulación. Tal como sucedió con "Tay", el *chatbot* de Microsoft que aprendía de lo que se hablaba en las redes sociales y, en tan solo un día de puesto en circulación, tuvieron que desconectarlo ya que se convirtió en un algoritmo neonazi racista enloquecido por el sesgo[39].

Lamentablemente, por más loable que consideremos la creación de principios y comités éticos, lo cierto es que, en la medida que aquellos no sean vinculantes, su efectividad será cuasi nula. Sin embargo, debemos celebrar que en octubre de 2020 en la Unión Europea se aprobó el informe de iniciativa legislativa donde se recomienda que la Comisión establezca un reglamento de principios éticos, globales y con visión de futuro para el desarrollo, el despliegue y el uso de la IA (entre otras tecnologías). Allí se determina que los sistemas de alto riesgo (como los analizados en este trabajo) deben ser imparciales, no discriminar por motivos de raza, sexo, orientación sexual, embarazo, discapacidad, características físicas o genéticas, edad, minoría nacional, origen étnico o social, lengua, religión o creencias, opiniones políticas o participación cívica, nacionalidad, estado civil o económico, educación o antecedentes penales. Previendo además instancias de evaluación de los riesgos y de conformidad con los sistemas y, en caso que esta última sea superada, se expedirá un certificado que lo valide.

38 Aristóteles. Ética a Nicómaco. Mestas Ediciones (2019).

39 Ver https://www.actionsdata.com/blog/lecciones-sobre-lo-que-puede-salir-mal-en-ia-tay-el-bot-que-idolatraba-a-hitler.

No haremos un análisis pormenorizado y profundizado de cada uno de los principios y miramientos éticos que señalamos en este trabajo, pero por su objeto, sí creemos necesario detenernos a reflexionar sobre uno de los conflictos más grandes entre la ética y la aplicación de estos instrumentos, esto es, los sesgos que ostentan.

¿Qué es un sesgo? Pensémoslo como una tendencia, una inclinación, una subjetividad de quien acciona condicionado por sus prejuicios y percepciones propias de la realidad. Por la naturaleza de los sistemas que estamos analizando podemos tomar la acepción estadística del diccionario de la RAE, que lo define como un "error sistemático en el que se puede incurrir cuando al hacer muestreos o ensayos se seleccionan o favorecen unas respuestas frente a otras". Es decir que un sesgo implica un proceso deliberativo, formar una opinión o un juicio. ¿Las máquinas tienen esa capacidad? No perdamos de vista que por más objetiva que se pretendan, estas herramientas son creadas y programadas por humanos con orientaciones y concepciones propias bien diversas. Esto quiere decir que todos esos prejuicios que tenemos por naturaleza se encuentran infiltrados en los datos de los cuales "aprende" el sistema, sumados a aquellos sesgos propios del desarrollador de la herramienta.

Respecto de los primeros, nos referimos a los sesgos que vienen inmersos en los datos con los cuales entrenamos el algoritmo. Llevemos nuestra mente a uno de los sistemas de policía predictiva. Los datos que se introducen en el software son los propios registros históricos generados por los oficiales, quienes sabemos que tienen una inclinación a patrullar determinadas zonas marginales de las sociedades en donde sospechan que encontraran más criminales. No podemos descartar que cuando el sistema es entrenado con esos datos, ese sesgo también es contagiado, generando un "bucle de retroalimentación pernicioso" que lleva a que los oficiales patrullen una y otra vez los mismos lugares (O'Neil, 2016[40]). Ahora supongamos que una de las personas detenidas a raíz de una predicción del sistema es absuelta: ¿el dato histórico de esa detención equivocada permanece en el sistema? Si la respuesta a esa pregunta es afirmativa, las futuras predicciones serían consecuencia de una falsa premisa.

Por otro lado, sería una ingenuidad descartar que los desarrolladores "moldean" los programas impregnándoles -de forma consciente o inconsciente- sus propios sesgos. La Comisión Europea ya puso de manifiesto que la falencia en la robustez y transparencia de los sistemas aumentan el riesgo de que reproduzcan, amplifiquen o alimenten sesgos de género de los que los programadores no sean conscientes o que son el resultado de una selección de datos específicos[41].

Un ejemplo claro son las herramientas de reconocimiento facial que, tal como se advirtió en un informe elaborado por la United Nations Development Programme[42], por el entrenamiento sesgado que reciben, pueden tener mucha menos precisión al identificar mujeres o rostros de piel oscura. De allí que distintas organizaciones europeas y latinoamericanas remarquen constantemente los riesgos que acarrean estos programas de IA para los derechos fundamentales de los ciudadanos.

La consecuencia temida es que esas herramientas, que son construidas e interpretadas por humanos, reproduzcan desigualdades injustificadas y ya existentes en el sistema de justicia[43]. Ello determina que, en lugar de

40 Cathy O'Neil. (2016). *Armas de destrucción matemática*.

41 *Informe Una Unión de la Igualdad: Estrategia Europea para la Igualdad de Género 2020-2025*, accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0152.

42 El informe se titula *Tackling Social Norms. A game changer for gender inequalities*. Accesible en http://hdr.undp.org/sites/default/files/hd_perspectives_gsni.pdf.

43 European Commission for the Efficiency of Justice (CEPEJ).

corregir ciertas problemáticas políticas y desigualitarias, se legitimen a través de esta tecnología, sobre todo porque tenemos la idea -equivocada- de que aquella no yerra y es plenamente objetiva[44].

VI. Prisa por dar respuestas, + interés por hacerlas preguntas correctas

No hay conclusiones en este trabajo pues no era el objetivo que nos propusimos cuando lo pensamos. Estas páginas son más bien un punto de partida. Creemos que era necesario generar un catálogo de algunas de las herramientas de IA que ya están siendo utilizadas hoy en día para prevenir e investigar conductas delictivas. Somos conscientes que quedaron algunos sistemas por mencionar, especialmente aquellos que asisten a los jueces en la toma de sus decisiones, como es el caso de COMPAS, que también ha sido objeto de duras críticas por sus sesgos (Dupuy, 2020[45]).

No es novedad que el crimen está en alza y que se ha sofisticado. También estamos convencidos de que la utilización de nuevas tecnologías es indispensable para combatirlo e intentar frenarlo. Nos generamos una desventaja enorme si no utilizamos su capacidad por pretender de ella una perfección utópica y nivel de exigencia superior al que tenemos con los operadores humanos. Pero tampoco podemos enceguecernos y blandir una navaja con dos filos con gran capacidad para lastimarnos.

Como siempre, el desafío es encontrar el punto medio que nos permita implementarlas con confianza pero sin aspiraciones surreales de eficacia. Lo que necesitamos no es certeza de resultados, sino de que los programas se están desarrollando con la finalidad genuina de mejorar el estado en el que como sociedad nos encontramos, no de incrementar los patrimonios de las compañías o elevar el valor de sus acciones en el mercado.

Si tenemos pruebas de que en la creación e implementación de la IA se vela por el respeto a las garantías de los ciudadanos, de que hay un marco regulatorio mínimo que incita a mejorar cada día la seguridad de aquello en lo que estamos innovando, de que se da intervención a todos los sectores involucrados, de que hay una conformación diversa (racial, religiosa, de género, etc.) en los grupos de desarrollo y trabajo, y que no se desoyen las directrices de los expertos consultados, esa fiabilidad en el proceso nos permitirá aceptar los errores que se produzcan sabiendo que serán necesarios para seguir aprendiendo, puliendo y mejorando.

Un exceso de teorización, reflexiones éticas y legislación sin la puesta en práctica no nos llevará a ningún lado. Para encontrar ese balance creemos que no es necesario sacar el pie del acelerador, pero sí bajar un cambio, dejar de buscar todas las respuestas de inmediato, sin saber si nos hicimos todas las preguntas correctas de antemano. Ese será el objetivo del próximo trabajo.

"European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment". Accesible en https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

44 Para más información se puede acceder al *Libro blanco sobre la Inteligencia Artificial* en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf y a la campaña #ConMiCaraNo de la ADC en https://conmicarano.adc.org.ar.

45 Dupuy, Daniela. Inteligencia Artificial y tecnologías disruptivas en el proceso penal. En *Inteligencia Artificial, Tecnologías Emergentes y Derecho*, Dir. Cecilia Danesi, Hammurabi (en edición).