ESTUDIOS BREVES

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO LEGAL

SONIA REGUEIRO LEMOS

Abogada | Universidad de Vigo

«*La inteligencia artificial es la ciencia e Ingeniería que permite diseñar y programar máquinas capaces de llevar a cabo tareas que requieren inteligencia para ser llevadas*»[1], o lo que es lo mismo, la inteligencia artificial (IA) es el campo de la informática cuyo objetivo es crear sistemas a través de los que puedan realizarse tareas que normalmente requieren inteligencia humana. Fue el Ministerio de Ciencia, Innovación y Universidades quien, en 2019, se aventuró a pronunciarse sobre este concepto tan difícil de definir como de comprender.

Bien es cierto que, a pesar de que hoy en día la IA se encuentre en nuestras conversaciones diarias, en las noticias o en las redes sociales, fue ALAN TURING quien se consagró como padre de esta tecnología en 1950. A través de su artículo *Computing Machinery and Intelligence*, introduce el conocido Test de Turing o lo que se conoció también como «*juego de la imitación*», a través del cual quería dar respuesta a la siguiente cuestión: ¿las máquinas pueden pensar?[2] TURING

describe este test como un simple juego en el que participan tres personas: un jugador que actúa como juez y que se encuentra en una habitación aislada y en otra habitación diferente estará un segundo jugador y una máquina que ha de hacerse pasar por un humano. Tanto la máquina como el segundo jugador tendrán que responder a las preguntas planteadas por el juez, con el objetivo de que éste no sea capaz de distinguir quien es el ordenador y quien el humano. Se considera entonces que, en los casos en los que hacer esta distinción sea tarea imposible la máquina ha alcanzado la suficiente inteligencia como para decir que las máquinas sí pueden pensar[3].

No obstante, han sido muchos los autores quienes se han pronunciado sobre el funcionamiento de este

campo de la tecnología, queriendo demostrar que lo que en la década de los 50 fue un adelanto, con el paso de los años no dejaba de ser un estudio altamente alejado de la IA como del funcionamiento del cerebro humano y de la neurociencia. Investigadores y científicos como el astrofísico STEVEN HAWKING incluso defendieron la teoría de que su falta de control podría conducirnos a efectos catastróficos[4]. Hoy en día se sabe que nos encontramos ante un potencial ilimitado en el desarrollo de la tecnología y que en la era digital actual es aplicable en multitud de áreas, llegando incluso a convertirse en uno de los aliados más potentes para los delincuentes, más en concreto para los ciberdelincuentes. La integración de la IA en los ciberataques ha aumentado con el paso de los años, incrementando tanto su complejidad como su eficacia. Los encargados de ejecutar los ataques acuden a mecanismos basados en esta tecnología para realizar toda una serie de prácticas con las que consigan una suplantación de la identidad o «*spoofing*», la creación de *deepfakes* o el desarrollo del más conocido como *phishing*, entre muchas otras prácticas ilegales empleadas por estos[5].

Un ataque por suplantación de identidad es uno de los peligros digitales que afecta a un alto número de personas y de organizaciones; los atacantes consiguen obtener todo tipo de información personal y valiosa después de realizar un estudio minucioso de la víctima[6]. A pesar de que parezca una tarea ardua, las herramientas que proporciona la IA facilitan a los atacantes un gran abanico de posibilidades para crear identidades artificiales mediante elementos reales y ficticios y a través de las cuales realizar todo tipo de prácticas ilegales que, a priori, parecen estar dentro de la más estricta legalidad. Dentro de este tipo de ciberataque uno de los más peligrosos es el conocido como *spoofing facial* o robo de la identidad digital, acto que se refiere a la suplantación de la identidad de una persona empleando su cara y simulando su biometría facial[7].

Partiendo de la base que el reconocimiento facial es uno de los mecanismos tecnológicos más empleados para el acceso a aplicaciones, sistemas o servicios, es de esperar que también sea una de las herramientas más empleadas por los ciberdelincuentes a la hora de querer ejecutar sus ataques. Desde un punto de vista general esta tecnología se basa en identificar automáticamente

a una persona mediante el análisis y la comparación de una imagen con los rasgos faciales y geométricos de la misma, como la distancia entre sus ojos, el contorno de sus labios, orejas y barbilla y de esta forma poder identificar los puntos principales y de referencia con los que se diferencia a un individuo de otro[8]. Desde esta perspectiva resulta difícil comprender cómo los delincuentes pueden reemplazar el rostro de la víctima y así acceder a cuentas bancarias, cuentas personales e incluso solicitar préstamos fraudulentos, no obstante, a través de la IA se comprobó que se podrían crear caras ficticias y neutras con las que los delincuentes pudiesen burlar los sistemas de seguridad del reconocimiento facial de los dispositivos electrónicos[9].

En segundo lugar, otra de las prácticas más empleadas y que ha supuesto un gran número de ciberataques es el conocido como *deepfakes* o «*falsedades profundas*», que consisten en crear videos, imágenes o audios con los que se recree en 3D la apariencia o el sonido de las personas. Estas réplicas se crean a través de las denominadas «*redes neuronales generativas antagónicas, GAN*»[10], es decir, mediante el uso de algoritmos o sistemas software, sin necesidad de intervención humana. Los atacantes modifican los rasgos de una persona haciéndola pasar por otra, generando de esta forma una confusión y una manipulación intencionada de las masas. Si bien es cierto los *deepfakes* se llevan empleando a lo largo de la historia en múltiples y diferentes áreas de actuación, siendo el cine para adultos uno de los principales escenarios en el que los ciberdelincuentes pueden sacar el máximo provecho de esta práctica[11].

A pesar de que la mayor parte de los atacantes empleen sistemas sofisticados para replicar tanto a famosos, políticos o incluso a pequeños empresarios, crear realidades falseadas está al alcance de cualquiera, en los últimos años se han creado aplicaciones gratuitas que permiten editar imágenes o videos de forma sencilla y cuyo resultado impide saber si estamos ante un *deepfake* o no, ya que como apuntan muchos estudios los resultados pueden ser extremadamente realistas. Lejos de las consecuencias inofensivas que puede generar el uso de estas aplicaciones accesibles a todo el público, el verdadero riesgo aparece cuando estas prácticas son empleadas con el objetivo de ofender, vulnerar el honor, la identidad o la imagen de las personas; así como también para generar confusión entre el público, riesgos que se seguirán viendo en la práctica como consecuencia de la inexistencia de una regulación efectiva que castigue y pene todas estas conductas contrarias a la Ley.

Por último, en relación con las prácticas ilegales usadas por los ciberdelincuentes hay que mencionar la que sin duda se ha configurado como una de las más dañinas y que, potenciada por el uso de las nuevas tecnologías se está volviendo de cada vez más empleada y recurrida por los estafadores. El *phishing*, o suplantación de la identidad, es la técnica con la que los atacantes, a través de mensajes, correos electrónicos, llamadas o sitios *webs* fraudulentos, engañan y manipulan a sus víctimas para que éstas descarguen programas falsos, compartan información personal o realicen actuaciones con las que expongan datos de ellas mismas y que de este modo, los delincuentes puedan realizar el ataque. Asimismo, cabe mencionar que esta práctica reviste distintos modos de actuación. Una de sus formas más habituales es a través de correos electrónicos masivos, de esta forma el estafador crea mensajes sobre temas creíbles y coherentes con los que engañar a los destinatarios resulta sencillo, consiguiendo que las víctimas descarguen archivos que infectan el dispositivo electrónico con el que acceden o divulguen información confidencial[12]. Si bien es cierto, a pesar de que ésta sea su forma habitual puede presentarse de muchas otras maneras: *vishing* o suplantación de identidad por teléfono; *smishing* o suplantación por mensajes de texto o *pharming* con el que redirige a las víctimas a sitios *webs* falsos[13].

A la vista está que, en un mundo donde los avances tecnológicos y el uso de la inteligencia artificial evoluciona sin dar tregua, de cada vez es más notoria la necesidad de crear una regulación que nos ampare y nos proteja de los ataques de los que nos acabamos convirtiendo en víctimas. Analizando esta cuestión, si la estudiamos en un primer momento a pequeña escala hay que mencionar que todavía existen muchos espacios donde las leyes existentes aún no son capaces de llegar, lo cual favorece que muchos de los atacantes, estafadores o ciberdelincuentes encuentren en estas lagunas legales las maneras idóneas para vulnerar cualquiera de nuestros derechos, que como se ha querido demostrar, están en peligro a diario. Uno de los

mecanismos con el que contamos para hacer posible un tratamiento y una protección de los datos personales y del desarrollo de la IA es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos (LOPD), Ley que en su artículo 28 establece las bases y las obligaciones que los responsables del tratamiento de los datos han de cumplir en todo momento para que, en caso de que se emplee la IA, los datos personales u análogos queden protegidos mediante la aplicación de esta normativa y que en relación con el precepto 82, del mismo texto legal, se reconoce el derecho que tienen los usuarios a la seguridad de las comunicaciones que transmitan y reciban a través de internet[14].

Asimismo, a modo de ejemplo y como forma para demostrar la falta de legislación con la que poder actuar frente a los ataques de los ciberdelincuentes, en relación con la suplantación de identidad en internet no existe un precepto legal que ofrezca una protección plena frente a este delito. Si bien es cierto, en el Código Penal se reconoce, en el artículo 401 CP, el delito de la usurpación del estado civil quedando libre de protección muchos otros supuestos que resultan necesario amparar, entre ellos todo lo que tiene que ver con el uso de la IA y de los medios tecnológicos para hacerse pasar por otra persona con el fin de generar daños personales o patrimoniales[15]. Con la entrada en vigor de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, más conocida como la Ley sí, sólo es sí, se introdujo en la disposición final cuarta una modificación del artículo 172.ter del CP, incluyendo un nuevo apartado en el que se hace mención, por primera vez, al uso incorrecto de las redes sociales como método delictivo[16]. Es importante destacar que, a pesar de que se incluya una condena para las conductas que utilicen la imagen de una persona sin su consentimiento para abrir perfiles falsos en redes sociales o en páginas que tengan una importante difusión pública, son muchas las prácticas delictivas que quedan sin castigo alguno, prácticas que son de cada vez más usadas por los ciberdelincuentes para acceder a todo tipo de datos y con las que poder realizar cualquiera de los ataques de los que se han mencionado, entre muchos otros. Esto es sólo un ejemplo de las lagunas legales que existen todavía en nuestro país y de la necesidad, cada vez más palpable, de crear normativas con las que poder limitar los ciberataques.

Sensu contrario, y como consecuencia del aumento considerable del uso de las tecnologías en los últimos años, concretamente a partir de la COVID-19, y de los riesgos e impactos negativos que lleva aparejado su uso, a nivel Europeo se aprobaron y se presentaron diferentes textos y proyectos normativos con los que se pretende establecer una serie de medidas con las que poder garantizar un elevado nivel de protección en el ámbito de la ciberseguridad. Por un lado, la Directiva sobre seguridad de las redes y sistemas de información (NIS2)[17], que entró en vigor en 2023 y con la que se actualizó la Directiva SRI2. Con ésta se pretende introducir nuevas normas con las que poder mejorar y avanzar a nivel comunitario en el ámbito de la ciberseguridad, tanto es así que con el objeto de aumentar la seguridad de los productos digitales la Comisión Europea presentó, el proyecto de ley de ciberresiliencia[18], aprobado por el Comité de Industria, Investigación y Energía, que tiene como finalidad proteger y mejorar la seguridad de los dispositivos empleados tanto por consumidores y empresas con los que compran o emplean programas informáticos en la era digital actual, es decir, con el propósito de ley se pretende responsabilizar a los vendedores y a los proveedores obligándolos a ofrecer actualizaciones en los sistemas informáticos para poner fin a todo tipo de vulnerabilidades y brindar una mayor seguridad al consumidor final[19].

Por otro lado, y en relación directa con el avance tecnológico, la Unión Europea está a punto de aprobar y de hacer oficial la primera regulación sobre IA con la que se sentarán las bases para garantizar el desarrollo de una tecnología e IA segura, ética y digna de confianza[20]. Con ésta se pretende establecer un amplio abanico de objetivos que pueden ir desde los más generales entre los que destacan la protección de la privacidad de los individuos[21], evitando de esta forma la recopilación, almacenamiento y utilización de datos personales con los que poder vulnerar la privacidad de las personas o la salvaguardia y protección de los seres humanos y de sus derechos, imposibilitando la creación de bases de datos o de aplicaciones con las que se vea favorecido cualquier tipo de injerencia o discriminación de los particulares[22]. Desde un enfoque más específico con este proyecto de Ley también se pretende establecer una serie de medidas con las que poder garantizar un elevado nivel de protección en el ámbito de la ciberseguridad, todo ello mediante un sistema de categorización en el que las plataformas de la IA se clasificación en atención al riesgo inherente que supone su uso y su afectación al bienestar social:

- Riesgo mínimo: aquellas plataformas cuyo uso supone un riesgo mínimo o nulo para la sociedad, como por ejemplo los spam basados en IA.
- Riesgo limitado: aplicaciones y servicios cuyo funcionamiento informa al usuario que está interactuando con un sistema de IA. Son plataformas que tienen la obligación de garantizar una transparencia con el consumidor final.
- Alto riesgo: aplicaciones y plataformas cuyo funcionamiento se basa en el cumplimiento de obligaciones legales más estrictas. Además, requieren de una supervisión humana para evitar cualquier tipo de problema, injerencia o vulneración de los derechos de los usuarios finales. Por ejemplo: los sistemas para el otorgamiento de créditos.
- Riesgo inaceptable: incluye todos los sistemas que su uso queda prohibido en la UE. Por ejemplo: los sistemas de puntuación de los gobiernos.

La tecnología avanza y los derechos de los usuarios quedan desprotegidos ante las muchas prácticas delictivas, en relación con la IA, que se ponen en práctica por atacantes, estafadores o delincuentes. Resulta necesario e incluso podría decirse que, imprescindible, crear tanto a nivel comunitario como a nivel nacional, una normativa capaz de proteger de forma eficiente el bienestar social, sin que los seres humanos queden desamparados y sin saber a qué norma acogerse para proteger sus derechos ante los ataques tecnológicos e informáticos, en los que acaban convirtiéndose en víctimas.

Referencias:

[1] PARDIÑAS REMESEIRO, S., «Inteligencia Artificial: un estudio de su impacto en la sociedad», A Coruña 2019-2020.

[2] «Maquinaria computacional e Inteligencia», Alan Turing, 1950. Traductor: Cristóbal Fuentes Barassi, 2010, Universidad de Chile.

[3] GARRIDO COUREL, M., «El test de Turing o la inteligencia de las máquinas», Madrid, 2014. https://www.eldiario.es/tecnologia/diario-turing/test-

turing-inteligencia-maquinas_1_5043307.html.
[4] DOUGLAS HEAVEN, W., «El test de Turing es una de las peores cosas que le ha pasado a la IA», 2021, https://www.technologyreview.es//s/13289/el-test-de-turing-es-una-de-las-peores-cosas-que-le-ha-pasado-la-ia.
[5] FERRÉ, X., «Cómo la inteligencia artificial está cambiando la ciberdelincuencia», 2023, https://www.ey.com/es_es/cybersecurity/como-la-inteligencia-artificial-esta-cambiando-la-ciberdelincuencia.
[6] «Qué son y cómo funcionan los ciberataques de suplantación de identidad», CIBERSEGURIDAD Y RIESGOS DIGITALES, https://www.ealde.es/ataques-de-suplantacion-de-identidad/.
[7] «La suplantación de identidad o spoofing: qué es y cómo prevenirlo», https://www.electronicid.eu/es/blog/post/spoofing-facial-que-es-como-prevenirlo-y-soluciones-de-deteccion-de-suplantacion-de-identidad/es.
[8] «Alertan por la estafa de la cara falsa», 2023, https://mundocontact.com/alertan-por-la-estafa-de-la-cara-falsa/.
[9] VÁZQUEZ, D., «Apenas 9 caras generadas con IA bastan para suplantar más de la mitad de las identidades de amplias bases de datos», 2021, https://www.businessinsider.es/decena-caras-generadas-ia-pueden-suplantar-identidad-911137.
[10] «Qué es un Deep fakes, cómo se crean, cuáles fueron los primeros y su futuro», 2021, https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros#:~:text=Un%20deep%20fake%20es%20un,profundo)%2C%20que%20utilizan%20algoritmos%20de.
[11] GONZALO, M., «Caso Almendralejo: los ´deepfakes` pornográficos y qué puede hacer la ley para proteger a las mujeres», 2023, https://www.newtral.es/deepfakes-pornograficos-mujeres-ley-ia-almendralejo/20230920/.
[12] «¿Qué es el phishing?», https://www.ibm.com/es-es/topics/phishing.
[13] «Phishing» o suplantación de identidad, https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/suplantacion-de-identidad.html.
[14] Inteligencia Artificial: un importante desafío legal para la privacidad y los derechos fundamentales, 2023, https://mascalvet.com/inteligencia-artificial-un-importante-desafio-legal-para-la-privacidad/.
[15] JOSÉ PELÁEZ, F., «El nuevo artículo 172 del Código criminalizará la suplantación de identidad en internet», 2022, https://www.economistjurist.es/articulos-juridicos-destacados/el-nuevo-articulo-172-del-codigo-penal-criminalizara-la-suplantacion-de-identidad-en-internet/.
[16] SÁNCHEZ, L., «La suplantación de identidad en internet que genere acoso o humillación a la víctima tendrá reproche penal», 2022, https://www.economistjurist.es/articulos-juridicos-destacados/la-suplantacion-de-identidad-en-internet-que-genere-acoso-o-humillacion-a-la-victima-tendra-reproche-penal/.
[17] Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2), Configurar el futuro digital de Europea, COMISIÓN EUROPEA, https://digital-strategy.ec.europa.eu/es/policies/nis2-directive.
[18] Ley de ciberresiliencia de la UE, Configurar el futuro digital de Europa, COMISIÓN EUROPEA, https://digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act.
[19] INCIBE., «La Comisión Europea presenta una nueva propuesta de resiliencia cibernética», 2023, https://www.incibe.es/empresas/blog/la-comision-europea-presenta-una-nueva-propuesta-de-resiliencia-cibernetica.
[20] GONZÁLEZ, F., «El Parlamento Europeo aprueba el proyecto de Ley para regular la inteligencia artificial», 2023, https://es.wired.com/articulos/parlamento-europeo-aprueba-el-proyecto-ley-para-regular-la-ia.
[21] Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, COMISIÓN EUROPEA.
[22] Europa marca el camino: ¿Será esta Ley de Inteligencia Artificial el modelo a seguir?, https://impulso06.com/europa-marca-el-camino-sera-esta-ley-de-inteligencia-artificial-el-modelo-a-seguir/.