

La IA ofrece oportunidades para el desarrollo, al tiempo que plantea desafíos éticos, jurídicos y sociales. En Marruecos, el marco jurídico está en plena evolución para tratar de responder a estos retos.

Amine Haoumani es doctorando en Ciencias Jurídicas, facultad de Ciencias Jurídicas y Políticas, Universidad Hassan I, Settat (Marruecos). Artículo original publicado en la *Revue Internationale de la Recherche Scientifique* (Revue-IRS) en junio de 2024.

LA INTELIGENCIA ARTIFICIAL EN MARRUECOS: ENTRE LA ÉTICA Y LA REGLAMENTACIÓN

La inteligencia artificial (IA) y las tecnologías afines ofrecen oportunidades decisivas para Marruecos, sobre todo en sectores clave como la agricultura, la salud y la educación. Sin embargo, también plantean desafíos éticos, jurídicos y sociales, sobre todo con respecto a la protección de los datos personales, la transparencia de los algoritmos y la responsabilidad en caso de disfuncionamientos. En ausencia de un marco normativo específico, es necesaria una reglamentación estricta para prevenir prácticas intrusivas y discriminatorias.

Marruecos, que ya se ha comprometido a poner en marcha un marco institucional, trasponer la recomendación de la UNESCO sobre la ética de la IA en sus estructuras, respaldado por la creación de un Centro de categoría II para la IA en África, bajo los auspicios de la UNESCO desde noviembre de 2023. No obstante, el país debe desarrollar una estrategia nacional de competencias y favorecer el consenso en torno a una visión ética y reglamentada de la IA para garantizar una integración inclusiva de esta tecnología.

La protección de los datos personales es un pilar esencial, con leyes

(nº09-08 y nº 05-20) que imponen obligaciones estrictas a las empresas e instituciones. La Comisión Nacional de Control de Protección de Datos de Carácter Personal (CNCP) asegura la supervisión de estas normas, pero persisten los retos en el ámbito de la transparencia algorítmica y el respeto a los derechos de los ciudadanos. Es necesario reforzar el marco legislativo para garantizar las explicaciones transparentes y evitar las discriminaciones.

Marruecos podría inspirarse en las mejores prácticas internacionales, como el RGPD (Reglamento General de Protección de Datos) en Europa, para integrar los principios de transparencia, limitación de finalidades y minimización de datos en su marco jurídico. El marco institucional desempeña un papel esencial, pero una colaboración estrecha entre reguladores, empresas y ciudadanos resulta primordial para garantizar una transición tecnológica ética y beneficiosa para todos.

¿Cuáles son los fundamentos necesarios para la elaboración de un marco jurídico y ético adaptado con el fin de guiar el uso de la inteligencia artificial en Marruecos?

DESAFÍOS ÉTICOS INHERENTES A LA INTELIGENCIA ARTIFICIAL

La integración de la IA en la sociedad marroquí presenta una serie de desafíos éticos y jurídicos muy importantes, sobre todo en materia de protección de datos personales. La explotación masiva de los datos para los sistemas de IA puede amenazar la vida privada si no se ponen en marcha medidas adecuadas y capaces de garantizar la seguridad y prevenir los abusos. Además, la transparencia de los algoritmos sigue siendo un problema crucial, dado el impacto tan significativo de las decisiones automatizadas sobre los individuos. Así, resulta esencial lograr que estos procesos de toma de decisiones sean comprensibles, a fin de preservar la confianza del público y prevenir todo rastro de parcialidad.

La equidad constituye, asimismo, un desafío primordial, puesto que los sistemas de IA corren el riesgo de reproducir o agravar los sesgos existentes en los datos empleados, lo cual podría dar paso a varias formas de discriminación. Para solucionarlo, es indispensable integrar los mecanismos de identificación y corrección de los sesgos. Dichos retos exigen un enfoque proactivo, basado en un

marco jurídico sólido y unos principios éticos definidos, con el fin de asegurar un uso responsable, equitativo y respetuoso de los derechos fundamentales de la IA en Marruecos.

LA PROTECCIÓN DE LA VIDA PRIVADA Y LOS DATOS PERSONALES EN LA ERA DE LA IA

La IA se asienta en el uso de unos vastos conjuntos de datos necesarios para el entrenamiento, el perfeccionamiento y el funcionamiento de los algoritmos. Esta dependencia intrínseca presenta una serie de retos fundamentales concernientes a la protección de la vida privada y la confidencialidad de la información personal. Los sistemas de IA, al recabar datos sensibles como los relacionados con la salud, las finanzas o las preferencias personales, ofrecen oportunidades de mejorar los servicios y productos, al tiempo que exponen a los usuarios a riesgos de abusos o violaciones. Para prevenir dichos riesgos, es esencial adoptar medidas como la minimización de los datos recabados, su anonimización y seudonimización o una gestión estricta del acceso. Por otra parte, el respeto a los marcos jurídicos en vigor, como el RGPD en Europa y la Ley 09-08 en Marruecos, se convierte en imperativo. La transparencia sobre la recogida y el uso de los datos, combinada con un control efectivo otorgado a los individuos sobre la información relacionada con ellos, constituye un pilar ético para garantizar su protección.

Más allá de las cuestiones de confidencialidad, surgen otros desafíos muy importantes, entre ellos el relativo a los sesgos algorítmicos. Cuando los sistemas de IA se entrenan a partir de conjuntos de datos sesgados, corren el riesgo de perpetuar o acentuar las discriminaciones. Así, la puesta en marcha de algoritmos transparentes y equitativos se revela como una necesidad. Además, las cuestiones de responsabilidad jurídica en caso de errores o daños causados por un sistema de IA deben clarificarse para asegurar una rendición de cuentas apropiada. Marruecos, al disponer ya de leyes como la 09-08 sobre la protección de datos personales y la 05-20 sobre ciberseguridad, debe reforzar su sistema jurídico para hacer frente a las especificidades de la IA. Si aborda estos desafíos mediante una reglamentación adaptada a las necesidades, una vigilancia constante y una colaboración

La transparencia en la recogida y el uso de los datos, combinada con un control efectivo sobre los individuos y la información relacionada con ellos, constituye un pilar ético para garantizar su protección

entre las partes interesadas, el país podrá garantizar un despliegue responsable y ético de la IA de acuerdo con los patrones internacionales y beneficioso para el conjunto de la sociedad.

LA TRANSPARENCIA DE LOS ALGORITMOS EN LA IA

En términos de transparencia de los algoritmos, las decisiones automatizadas por los sistemas de IA –ya sea con respecto a la concesión de créditos, los procesos de selección o la evaluación de riesgos en la justicia– suelen ser opacas y difíciles de interpretar. Ello puede comprometer los derechos fundamentales de los individuos, a la vez que plantea cuestiones importantes vinculadas a las entidades que emplean estas herramientas. El marco jurídico actual, sobre todo en materia de protección de datos personales, sigue siendo insuficiente para controlar estos procesos. Así, es imprescindible implantar reglamentaciones específicas que impongan la divulgación de los algoritmos y la explicitación de los criterios que llevan a la toma de decisiones. Una mayor transparencia reforzaría la confianza de los ciudadanos y limitaría los sesgos concernientes a la toma de decisiones.

En cuanto a la equidad, los algoritmos de la IA, a menudo entrenados a partir de datos sesgados, corren el riesgo de reproducir o acentuar las discriminaciones históricas, ya sea en el ámbito de la justicia, el empleo u otros sectores. Estos sistemas podrían favorecer o bien perjudicar a unos grupos a partir de criterios arbitrarios como su origen étnico o su género, lo cual llevaría a exacerbar las desigualdades sociales. Ante dicha amenaza, se imponen mecanismos de corrección que incluyan auditorías regulares de los algoritmos, la diversificación de los datos empleados y la integración de medidas específicas para atenuar los sesgos. Estas acciones deben acompañarse de reglamentaciones firmes que aseguren la equidad y prevengan toda forma de discriminación.

EVALUACIÓN Y DIAGNÓSTICO DEL ESTADO DE PREPARACIÓN A LA IA

Marruecos ha emprendido una ambiciosa andadura para ajustar su desarrollo de la IA a las recomendaciones éticas de la UNESCO, con el objetivo de maximizar las oportunidades y minimizar los riesgos, respetando los derechos fundamentales. El país lleva elaborando desde 2022 una cartografía de su ecosistema de IA que identifica las prioridades estratégicas para su desarrollo, sobre todo el refuerzo del marco regulatorio, la transparencia de los algoritmos, la protección de datos y la lucha contra los sesgos discriminatorios.

Marruecos también apuesta por una gobernanza multipartita y multidisciplinar que supervise la IA de manera ética y eficaz, así como por el desarrollo de las capacidades mediante la formación de una mano de obra cualificada y adaptada a las transformaciones producidas por la IA. La inclusión digital es otra prioridad, que implica una serie de esfuerzos para reducir las disparidades regionales y de género, así como para favorecer una IA accesible y equitativa. La estrategia *Digital Morocco 2030* apoya la innovación digital y las asociaciones entre usuarios, universidades y empresas, reforzando así las infraestructuras digitales.

Pese a los avances logrados, quedan aún desafíos, sobre todo en el ámbito de la política medioambiental para la IA, así como en lo referente a la preservación del patrimonio cultural y las lenguas autóctonas. Marruecos también debe subsanar las desigualdades de acceso a las tecnologías entre sexos y regiones. Sin embargo, el país dispone de bazas muy sólidas, entre ellas una base académica muy reforzada, con una tasa de feminización del 42,2% en las carreras científicas, y numerosas iniciativas de gobernanza digital muy avanzadas, como los proyectos de *smart cities*.

De este modo, Marruecos se sitúa como líder potencial en IA en el con-

tinente africano, con una visión que conjuga ética, innovación e inclusión apoyada por varios partenariados internacionales e inversiones en educación, investigación e infraestructuras digitales. Al conjugar la ambición con la responsabilidad, el país pretende explotar el potencial transformador de la IA respetando los valores de justicia y equidad.

EVALUACIÓN DEL MARCO JURÍDICO E INSTITUCIONAL

El aumento del poder del ciberespacio ha supuesto numerosos retos jurídicos y de seguridad a los que Marruecos, al igual que otros países, debe enfrentarse. El creciente uso de internet, redes sociales, comercio electrónico e IA ofrece oportunidades significativas, pero también expone a amenazas como la ciberdelincuencia, la violación de la vida privada y la explotación abusiva de los datos personales.

Para superar estos retos, Marruecos se ha involucrado en un proceso de refuerzo de su sistema jurídico e institucional. Este enfoque no se limita a la represión de las ciberdelitos, sino que también aspira a proteger los derechos digitales de los ciudadanos, sobre todo la libertad de expresión en internet, el acceso a la información y la neutralidad de la red, siempre preservando las identidades digitales de los usuarios.

Marruecos se apoya en una serie de leyes adoptadas a lo largo de las dos últimas décadas relacionadas con el ciberespacio, entre las que destacan:

—Ley 07-03, relativa a las infracciones vinculadas a los sistemas de tratamiento automatizado de datos (STAD).

—Ley 09-08, que atañe a la protección de datos personales.

—Ley 43-20, que concierne a los servicios de confianza para las transacciones electrónicas.

—Ley 04-20, que instituye el Documento Nacional de Identidad Electrónico (CNIE).

—Ley 53-05, relativa al intercambio electrónico de datos jurídicos.

—Ley 05-20, centrada en la ciberseguridad.

Este marco jurídico traduce la voluntad de las autoridades de garantizar un uso seguro y ético de las tecnologías digitales, a la vez que incentivar la innovación y reforzar la confianza de los ciudadanos y las empresas en el ecosistema digital.

Pese a todos estos progresos, la ausencia de un marco jurídico especí-

fico consagrado a la IA en Marruecos plantea desafíos importantes. Las leyes existentes ofrecen una base inicial, pero siguen siendo insuficientes para controlar las especificidades de la IA. En ausencia de regulaciones adaptadas, la IA puede usarse de forma no ética, lo cual engendra riesgos como la recogida y el tratamiento no reglamentados de datos personales, la discriminación y los sesgos algorítmicos en las decisiones automatizadas, la explotación incontrolada de los trabajadores del ámbito digital y la vulneración de la vida privada y la dignidad humana.

Esta laguna entorpece, asimismo, la innovación responsable, puesto que las empresas y los investigadores carecen de directivas claras sobre las normas que deben respetar. Además, puede limitar los atractivos de Marruecos en el escenario internacional en materia de inversión y desarrollo tecnológico.

■ Marco institucional

El desarrollo digital marroquí se asienta sobre numerosas instituciones clave, cada una de las cuales desempeña un papel fundamental en la puesta en marcha de la estrategia nacional y la regulación de las tecnologías digitales, así como la protección de los datos personales y la ciberseguridad.

—*La Agencia de Desarrollo Digital (ADD)* es la responsable de la ejecución de la estrategia nacional de desarrollo digital y actúa en favor de la adopción de tecnologías digitales por parte de los ciudadanos, las empresas y las instituciones. Entre sus funciones se incluye la estructuración del ecosistema digital para favorecer la emergencia de actores clave en la economía digital, el apoyo de la administración digital y la reducción de la brecha digital. La agencia también respalda la innovación social y relativa al emprendimiento, contribuyendo a una inclusión digital responsable y duradera.

—*La Agencia Nacional de Reglamentación de las Telecomunicaciones (ANRT)* asegura la regulación del sector de las TIC en Marruecos. Se encarga de la elaboración del marco reglamentario del sector, otorga las licencias necesarias a los operadores y gestiona recursos como el espectro de las frecuencias. La ANRT también vela por la calidad de los servicios y la promoción de la competencia legal, además de contribuir a la sociedad de la información a través de actividades de formación e investigación.

—*La Dirección General de Seguridad Nacional (DGSN)* es la responsable de la seguridad interna, sobre todo en los dominios de la ciberdelincuencia y la protección de datos personales. Se encarga de investigar infracciones vinculadas a la ciberseguridad, sensibiliza al público sobre los riesgos relacionados con la divulgación de datos personales y colabora con otras instituciones para identificar, investigar y perseguir a los ciberdelinquentes. También garantiza la seguridad de los sistemas de información de las instituciones públicas y los organismos gubernamentales.

—*La Dirección General de Seguridad de Sistemas de Información (DGS-SI)* despliega dispositivos de seguridad para proteger los datos personales y los sistemas de información críticos, además de establecer una estrategia nacional de seguridad de los sistemas de información en colaboración con los ministerios y otras partes interesadas. También elabora normas y patrones de seguridad para los sistemas que tratan datos personales, aconseja y asiste a entidades públicas y privadas y realiza auditorías de seguridad para identificar posibles focos de vulnerabilidad.

—*La Comisión Nacional de Control de Protección de Datos de Carácter Personal (CNDP)* vela por la conformidad de las prácticas de tratamiento de los datos personales según la Ley n°09-08, informa a los ciudadanos de sus derechos en materia de protección de datos, atiende las quejas y sensibiliza a los actores implicados acerca de sus obligaciones legales. Efectúa, asimismo, inspecciones para verificar la conformidad de los tratamientos de datos y gestiona las autorizaciones de tratamiento de datos sensibles.

—*El Centro Marroquí de Alerta y Gestión de Incidentes Informáticos (MA-CERT)* se encarga de la vigilancia y gestión de los ciberataques e incidentes informáticos. Coordina las acciones de respuesta a las amenazas digitales en el ámbito nacional, comparte información sobre las amenazas y los focos de vulnerabilidad con los organismos de ciberseguridad y sensibiliza al público y las empresas sobre la importancia de la ciberseguridad. Asimismo, contribuye a la formación y el refuerzo de las competencias en ciberseguridad.

—*El Comité Estratégico de Ciberseguridad (CSC)* coordina los esfuerzos para proteger los sistemas de información marroquíes contra las ciberamenazas.

zas, elabora políticas y normas de ciberseguridad, colabora con la Gendarmería Real para detectar y reprimir ciberdelitos y garantiza la seguridad de las infraestructuras públicas y privadas. El comité vela por la construcción de un ciberespacio seguro y resiliente para el país.

—*La Comisión Nacional para el Desarrollo Digital* supervisa la puesta en marcha de la estrategia nacional de desarrollo digital, formula recomendaciones y evalúa los progresos realizados en el marco de la estrategia digital. También organiza comisiones temáticas para abordar aspectos específicos del desarrollo digital y promueve la colaboración entre las autoridades públicas, los expertos y las partes interesadas.

—*La Célula Digital de la Secretaría General del Gobierno* supervisa la instauración de la estrategia digital en el seno del gobierno, apoyando la transición digital; regula y coordina las actividades digitales en el marco de la estrategia *Digital Morocco 2030*; asegura la creación de un marco jurídico para acompañar la transición digital y colabora con los actores públicos y privados para reforzar las infraestructuras digitales y la regulación del sector.

■ Puntos fuertes

El sistema jurídico marroquí concerniente al ciberespacio se asienta sobre un enfoque global cuyo objetivo pasa por supervisar las TIC. Se centra en varios aspectos clave: la protección de los datos personales, la lucha contra la ciberdelincuencia, la garantía de las transacciones electrónicas seguras y la promoción de la innovación tecnológica.

La protección de los datos personales viene reforzada por las obligaciones estrictas que tienen los responsables de su tratamiento y por un control asegurado por la CNDP. El marco jurídico también combate la ciberdelincuencia, definiendo infracciones específicas y reforzando los poderes de las autoridades para investigar y sancionar las actividades ilegales en línea.

Marruecos facilita las transacciones electrónicas a través de leyes que garantizan su validez y seguridad, respaldando así el crecimiento de la economía digital. La ciberseguridad también es prioritaria, con medidas de protección contra los ciberataques e iniciativas para hacer más seguros los sistemas de información críticos.

Finalmente, Marruecos alienta la innovación digital apoyando las *start-ups*

y la investigación tecnológica a la vez que sensibilizando a los usuarios con respecto a la ciberseguridad. La puesta en marcha de una plataforma nacional de identidad digital asociada al documento nacional de identidad electrónico aspira a reforzar la fiabilidad de las transacciones en línea.

Todos estos esfuerzos están llamados a crear un entorno digital seguro, fiable y propicio a la innovación, protegiendo los derechos de los usuarios y respetando las normas internacionales.

■ Lagunas

En Marruecos la protección de datos personales frente a la IA está regida por la Ley General sobre Protección de Datos. El objetivo de dicha legislación pasa por proteger los derechos individuales, pero se concentra, sobre todo, en los datos que permiten identificar a una persona. Sin embargo, la IA y los Big Data sobrepasan a menudo la gestión de los datos individuales para incluir datos agregados, perfiles genéricos y correlaciones estadísticas que, aunque no se consideren datos personales en el sentido más estricto, sí pueden influir en la vida de las personas. El marco jurídico actual parece insuficiente para responder a los desafíos planteados por el uso creciente de estas tecnologías, lo cual exige una evolución legislativa para incluir normas adaptadas a la realidad de la IA y los Big Data.

■ Recomendaciones

—*La ausencia de un marco jurídico que regule los Big Data*: en Marruecos, la protección de los Big Data se refiere a la reglamentación general relativa a la protección de las personas físicas de acuerdo con el tratamiento de datos de carácter personal (Ley 09-08), mientras que los datos masivos, a diferencia de los personales, no gozan de una protección jurídica específica. Así, constituyen un campo muy atractivo en materia de investigación e innovación en diversos dominios, lo cual justifica la implantación de un derecho prospectivo. La regulación en vigor se centra en intereses particulares y derechos fundamentales como la preservación de la vida privada y la protección de datos, basados en la noción de "datos personales" que permite identificar o caracterizar a una persona física. No obstante, los procesos que atañen a los Big Data trascienden la gestión única y el tratamiento de datos a escala individual, incluyendo el uso cre-

ciente de datos consolidados, perfiles generales y perfiles de grupo. A partir de este punto, conviene interrogarse acerca de la pertinencia del enfoque sobre el individuo y los datos personales en la era de los Big Data. Las correlaciones estadísticas y los perfiles de grupo no se reconocen como datos personales pese a su capacidad de influir ampliamente en el contexto de la vida de los individuos. Además, el crecimiento del uso de los Big Data plantea cuestiones sobre la definición misma de los datos personales.

—*La necesidad de una ley marco para regular la Inteligencia Artificial*: Hoy en día Marruecos no dispone de una legislación específica para regir la IA, lo cual crea un vacío jurídico y exige la adopción de una ley marco para asegurar un desarrollo ético y responsable de la IA. Esta ley debería definir los principios fundamentales, las normas de seguridad y los mecanismos de control, así como las responsabilidades de los actores implicados en el ecosistema de la IA. También debería contribuir a asegurar la protección de datos individuales, la transparencia y la confianza del público en esta tecnología en constante evolución.

—*El imperativo de respaldar la adopción de la nube en Marruecos*: aunque resulta innegable que la computación en la nube es uno de los avances tecnológicos más revolucionarios de nuestra época, en Marruecos aún no se ha adoptado plenamente. No obstante, alentar el uso de la nube ofrece innumerables ventajas, tanto para las empresas como para la administración pública. La nube permite una flexibilidad sin parangón, favorece la eficacia de las operaciones y reduce los costes informáticos. Por otra parte, permite el acceso a recursos informáticos de tecnología punta, abriendo camino a la innovación y la competitividad. Para maximizar estas ventajas, es indispensable poner en marcha una infraestructura legislativa y técnica adaptada. La seguridad, la protección de datos y la confidencialidad son preocupaciones esenciales en el contexto de la nube. En este entorno que no deja de evolucionar con gran rapidez, Marruecos tiene la oportunidad de estimular su crecimiento económico, modernizar su sector público y mejorar la calidad de vida de sus ciudadanos mediante una amplia adopción de la computación en la nube. Ya es hora de promover políticas e incentivos destinados a alentar a las empresas y los organismos públicos a abrazar esta tecnología. /