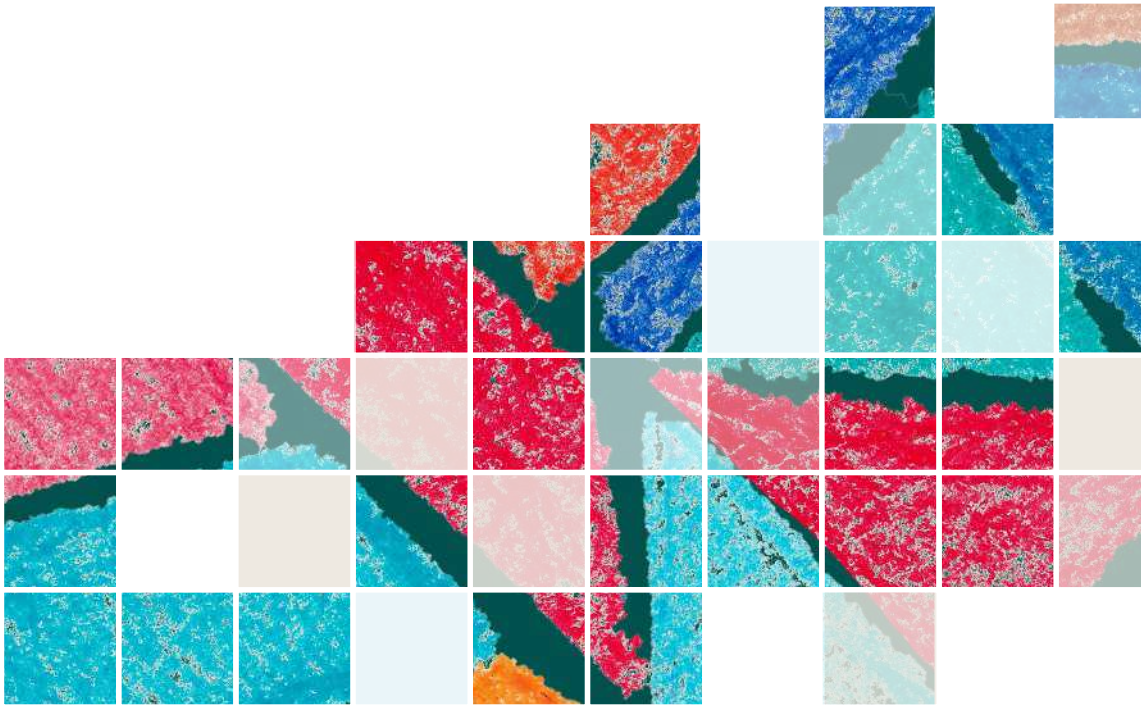
TEMAS

Introducción a la Ética y el Derecho de la Inteligencia Artificial

Coordinadora

Michelle Azuaje Pirela



LA LEY

Introducción a la Ética y el Derecho de la Inteligencia Artificial

uah / Facultad de Derecho
Universidad Alberto Hurtado

LA LEY

LA LEY Soluciones Legales, S.A.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
https://www.laley.es

Primera edición: marzo 2023

Depósito Legal: M-7777-2023
ISBN versión impresa: 978-84-19446-21-3
ISBN versión electrónica: 978-84-19446-22-0

Diseño, Preimpresión e Impresión: LA LEY Soluciones Legales, S.A.
Printed in Spain

3. REGULANDO EL RFA

3.1. Modelos de regulación del RFA

¿Cómo gobernar el uso del RFA? Las alternativas van desde la autorregulación privada hasta su prohibición. En este apartado se explican resumidamente algunos de los modelos para normar el empleo de esta tecnología.

3.1.1. Gobernanza ética del RFA

En primer término, el RFA podría quedar sometido simplemente a la corrección ética de sus desarrolladores y de quienes emplean estos sistemas. Esta opción no descansa en reglas jurídicas vinculantes, sino que confía en directrices o estándares éticos que pueden promover por la industria u otros sectores[(26)]. Los lineamientos éticos tienen impacto en el diseño, desarrollo, supervisión y auditoría de algoritmos de RFA.

La dimensión ética de la IA es uno de los grandes debates en la literatura comparada[(27)]. La gran ventaja de esta aproximación regulatoria es su ductibilidad ante el cambio tecnológico. Sin embargo, dada la falta de coercibilidad de sus directrices, se suele acusar que la apuesta por la gobernanza ética de algoritmos es una estrategia de lavado de imagen o *ethics washing*[(28)]. La gobernanza ética, como modelo exclusivo, parece estar llegando a su fin, particularmente en Europa[(29)].

Un ejemplo de este tipo de aproximación es el que observamos en el ámbito interamericano. A nivel del continente, la regulación no se encuentra en el mismo nivel de especificidad desarrollada por Europa, como se revisa en el siguiente apartado. De partida, no existe un tratado internacional que aborde, al menos en términos generales, la protección de datos personales. Por ello, sólo cuenta con instrumentos de *soft law* que abordan indirectamente el tipo de tratamientos de datos que efectúa un sistema de RFA. La Organización de Estados Americanos (OEA), a través de su Comité Jurídico Interamericano (CIJ), ha aprobado trece principios en materia de protección de datos personales, en su versión actualizada de abril de 2021. En el Principio 9 se reconoce la categoría de «datos personales sensibles» y fija las

(26) CONTRERAS & TRIGO (2021).
(27) MITTELSTADT *et al*. (2016).
(28) WAGNER (2018) 84-90, METZINGER (2019); WATTS (2019).
(29) FLORIDI (2021).

directrices para su tratamiento[30]. Conforme al criterio del CIJ, los datos biométricos se encontrarían en dicha categoría[31] y se recomienda a los Estados a establecer garantías especiales dentro de su legislación nacional, para así proteger los intereses de las personas en el ámbito de la privacidad y establecer la magnitud de la prohibición del tratamiento de datos personales sensibles y las excepciones a la misma[32]. Sin perjuicio de lo anterior, el instrumento no supone una fuente formal de derecho internacional ni su infracción generaría, por sí, un incumplimiento de una obligación internacional que comprometa la responsabilidad de los Estados miembros de la OEA.

3.1.2. Regulación a través de normas de protección de datos personales

En segundo lugar, existen aproximaciones regulatorias sectoriales, a partir de las leyes y marcos normativos de protección de datos personales. Dado que el funcionamiento del RFA supone un tratamiento de datos biométricos, un entorno regulatorio natural han sido las leyes y autoridades de control, en materia de protección de datos personales.

Por ejemplo, en el marco europeo, el Reglamento General de Protección de Datos («RGPD») define el concepto de datos biométricos y lo somete bajo su regulación[33]. Este tipo de datos son obtenidos a partir de un tratamiento especial[34] y que permiten la individualización *única* de la persona natural[35]. Conforme al art. 9 RGPD, se establece la prohibición general del tratamiento de categorías especiales de datos, lo que incluye los datos biométricos. Sin embargo, excepcionalmente se autoriza el tratamiento bajo diez

(30) «*Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos*». Véase, Los principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales, con anotaciones (2021).

(31) CJI (2021) 7-23.

(32) CJI (2021) 22-23.

(33) RGPD: «Art. 4. Definiciones. […] 14. "datos biométricos" datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos».

(34) En el entendido que efectúa una «medición» de las características especiales de la persona. Véase EUROPEAN DATA PROTECTION BOARD (2021) 19 y ss.

(35) Por tanto, las imágenes de video de una persona física no pueden considerarse a sí mismas datos biométricos, si no se han tratado específicamente para aportar en la individualización de la persona. EUROPEAN DATA PROTECTION BOARD (2021) 19.

hipótesis taxativamente enunciadas, entre las que se encuentra el consentimiento explícito del titular, la necesidad para cumplir obligaciones laborales y de seguridad social o cuando sea necesario por razones de un interés público esencial, entre otras causales (art. 9 RGPD). Nótese que el EDPB ha interpretado el responsable del tratamiento de datos no puede condicionar el acceso a sus servicios a la aceptación positiva del tratamiento biométrico, debiendo «ofrecer una solución alternativa que no implique el tratamiento biométrico, sin restricciones ni coste adicional para el interesado» (36).

Otro importante instrumento es el Convenio No. 108+ (37), el tratado internacional promovido por el Consejo de Europa en materia de datos personales, pero abierto a la firma por parte de cualquier Estado. En América Latina, sólo Argentina, México y Uruguay son Estados partes del tratado. Al igual que el RGPD, incorpora la categoría de datos especiales o sensibles, entre los que se incluyen los datos genéticos y los biométricos (art. 6.1 C. 108+) (38). Se trata de datos que tienen un marco de protección reforzado, puesto los Estados deben adoptar los resguardos necesarios y adecuados bajo su legislación nacional, con el objeto de prevenir los riesgos que el tratamiento de datos sensibles pueda presentar «para los intereses, derechos y libertades fundamentales» del titular o el «riesgo de discriminación» (art. 6.2 C. 108+). En materia de reconocimiento facial, las tecnologías de RFA solo pueden tener lugar en entornos controlados con fines de verificación, autenticación o categorización. Se procura garantizar este consentimiento mediante el otorgamiento de soluciones alternativas al uso de RF, tales como contraseñas, tarjetas de verificación, huella dactilar, entre otras opciones de uso fácil, de modo que la elección sea legitima (39).

3.1.3. Regulación a través de leyes especiales

En tercer lugar, encontramos leyes especiales que atacan directamente los efectos del RFA. En este modelo, la diversidad de alternativas y herramientas pueden ir desde prohibiciones específicas hasta condicionamientos para su utilización. Para ejemplificarlo, conviene revisar algunos casos de ciudades que han prohibido el uso de esta tecnología.

(36) EUROPEAN DATA PROTECTION BOARD (2021) 22.
(37) Convenio modernizado para la protección de las personas con respecto al procesamiento automático de datos personales es una adopción del protocolo modificativo CETS No. 223 para la modernización de la convención 108. Estrasburgo, 10 de octubre 2018. Véase COUNCIL OF EUROPE PORTAL (2021).
(38) COUNCIL OF EUROPE (2018) 8 y ss.
(39) COUNCIL OF EUROPE (2021).

San Francisco fue la primera ciudad que dictó una legislación especial sobre la materia[40]. Luego de ello, el modelo de prohibición se extendió a Oakland, Berkley y Sommerville (Mass.)[41]. En síntesis, el modelo de prohibición adopta una decisión distinta a la moratoria propiciada por la Alta Comisionada para los Derechos Humanos. El uso de RFA se encontraría proscrita en términos indefinidos, mientras que una moratoria suspende su empleo durante el plazo estipulado o la verificación del cumplimiento de las condiciones fijadas para ser validada. En el caso de San Francisco, el uso de RFA estaría proscrito para actividades de vigilancia local. Como se establece en los fundamentos de la «Stop Secret Surveillance Act», existe una «propensión de la tecnología de reconocimiento facial a poner en peligro los derechos y las libertades civiles [que] supera sustancialmente sus supuestas ventajas y la tecnología exacerbará la injusticia racial y amenazará nuestra capacidad de vivir libres de la continua vigilancia del gobierno»[42].

Otra alternativa regulatoria es la que se observa en el Estado de Washington. La ley SB 6280[43], sobre el uso de servicios de reconocimiento facial entró en vigor en julio de 2020 y que no prohíbe el empleo de RFA sino que fija condiciones y requisitos para su operación. Cabe hacer presente que el proyecto de ley fue patrocinado por el Senador estatal Joe Nguyen, quien actualmente trabaja como gerente de programas de Microsoft[44]. Uno de los elementos centrales es la obligación de los proveedores de tecnologías de RFA de proveer información relativa a sesgos o discriminación en el funcionamiento del sistema o en la prestación del servicio. La regulación introduce principios de transparencia y rendición de cuentas, así como la notificación pública de la finalidad para cual se empleará la tecnología. Por otro lado, establece medidas en contra de la vigilancia continua: «una autoridad pública no puede utilizar el reconocimiento facial para participar en vigilancia continua, realizar identificación en tiempo real o casi en tiempo real, o iniciar un seguimiento persistente». Sin embargo, se exceptúa de la prohibición si se cuenta con orden judicial previa para encontrar o identificar a una persona desaparecida o identificar a una persona fallecida o en casos de circunstancias apremiantes[45].

(40) CONGER *et al.* (2019).
(41) GARAY (2019) 4 y ss.
(42) STOP SECRET SURVEILLANCE ORDINANCE, §1(d).
(43) WASHINGTON STATE LEGISLATURE (2020).
(44) GERSHGORN (2020).
(45) SMITH (2020).

La Cuarta Revolución Industrial ha llegado para quedarse y para seguir transformando las sociedades y la economía mundial. Esta revolución digital acompañada de la inteligencia artificial (IA) y de otras tecnologías digitales emergentes, ofrece enormes oportunidades que ya pueden apreciarse en ámbitos tan diversos como: el transporte, el marketing, los servicios sanitarios, las finanzas, la seguridad, la educación, la asistencia personal, entre otros. Sin embargo, también emergen nuevos retos y desafíos para un sinnúmero de oficios y profesiones y, obviamente, el Derecho no es una excepción. El despliegue de la IA y su fusión con diversas tecnologías que interactúan a través de lo físico, digital y biológico, plantean nuevos paradigmas que requieren de profesionales con formación altamente especializada.

A lo largo de sus quince capítulos, este manual analiza desde una perspectiva nacional y comparada los principales riesgos y oportunidades que plantea el diseño e implantación de tecnologías de IA y el impacto que estas tienen o pueden llegar a tener en los derechos de las personas, así como las tendencias normativas frente a los desafíos ético-jurídicos de la transformación digital.

ISBN: 978-84-19446-21-3

LA LEY