URU
REVISTA DE COMUNICACIÓN Y CULTURA

Caso 700 IA: Entre la protección de datos personales y el uso de la inteligencia artificial

Case 700 AI: Between Data Protection and the Use of Artificial Intelligence

Recepción: 08/01/2024, revisión: 10/01/2024,
aceptación: 04/04/2024, publicación: 01/01/2025

https://revistas.uasb.edu.ec/index.php/uru

Daniel Fernando Mejía Terán
Investigador independiente
Quito, Ecuador
daniel.fernando.mejia@hotmail.com

https://doi.org/10.32719/26312514.2025.11.7

Resumen

El apogeo de las nuevas tecnologías ha captado la atención de los actores que participan en la sociedad global. En este contexto, un colegio de Quito se convirtió en una escena de reflexión y estudio sobre la interacción con la inteligencia artificial (IA) y la protección de datos personales. El desarrollo de este texto ofrece una travesía hacia el fenómeno de la globalización y de repensar el derecho como una ciencia transversal a la tecnología. La multidisciplinariedad es el enfoque de investigación que guiará la explicación de los conceptos desarrollados. Adicionalmente, se dará un vistazo al sistema de protección de datos personales en Ecuador, que aún no está completo y cuya vigencia es muy reciente. Es un desafío comprender la IA y la injerencia de la protección de datos personales en un Estado subdesarrollado y con escasa educación digital. Sin embargo, es loable tratar de crear un precedente académico —a partir del análisis del Caso 700 IA— que permita a la sociedad entender la realidad oculta por aquellos que aún no se adaptan a los nuevos cambios sociales de la globalización.

Abstract

The rise of new technologies has captured the attention of each of the actors who participate in a global society. The emergence of Artificial Intelligence (AI) can provoke countless reactions and actions. In this context, a school in Quito became the scene of reflection and study on the interaction with AI and the protection of personal data. The development of this text offers a journey towards the phenomenon of globalization and the rethinking of Law, as a science transversal to technology. Multidisciplinarity is the research approach that will guide the explanation of each of the concepts developed in the corresponding sections. Additionally, a look will be given at the personal data protection system in Ecuador, which is very recent in force, and is not yet fully complete. It is a challenge to understand Artificial Intelligence and the interference of personal

data protection in an underdeveloped State, with little digital education. However, it is commendable to try to create an academic precedent that allows society to understand, through the story behind the "700 AI Case", the reality hidden by those who have not yet adapted to the new social changes of globalization.

Palabras clave · *Keywords*
Inteligencia artificial, datos personales, imágenes, protección de datos personales
Artificial intelligence, personal data, images, personal data protection

Introducción

El 4 de octubre de 2023, en la mayoría de los medios de comunicación, se narraba un caso sobre el uso de inteligencia artificial (IA) para la creación de contenido sexual de estudiantes menores de edad inscritos en un colegio de la ciudad de Quito (El Universo 2023). Esta noticia captó la atención de distintos segmentos poblacionales, debido al contexto y la influencia de esta nueva tecnología, que cada vez es más popular en nuestra sociedad globalizada. Al estudiar este caso, saltan a la vista factores de análisis y reflexión; por ejemplo, los perpetradores del tratamiento ilegítimo de datos personales (imágenes) de las menores de edad eran jóvenes de bachillerato, en su mayoría compañeros de las víctimas. Adicionalmente, la cantidad de archivos de contenido sexual generados por medio de la IA, según la mayoría de las fuentes, era alrededor de 700, entre videos y fotografías (Loaiza 2023). Es por eso que para el desarrollo de este texto se lo ha denominado "Caso 700 IA", haciendo alusión a las siglas de *inteligencia artificial* y la cantidad impresionante de archivos generados.

El Caso 700 IA es un precedente nefasto para los procesos de regulación de la IA en Ecuador, y también para la protección de datos personales. En la construcción del marco fáctico de este caso, se puede observar como responsables del daño ocasionado a jóvenes de bachillerato, con edades entre los 15 y los 17 años, compañeros del colegio de las víctimas, también menores de edad. El acto o hecho, que repercutió en los derechos de privacidad y protección de datos personales de las víctimas, es la manipulación o el tratamiento de sus imágenes para la creación de contenido sexual por medio de la IA.

El método utilizado en el Caso 700 IA se denomina *deepfake*, y consiste en "un video que superpone la cara de una persona en el cuerpo de otra. Es posible gracias a algoritmos gratuitos y fáciles de usar. Se ha empleado, eminentemente, para crear videos pornográficos, con el rostro de actrices famosas" (Cerdán y Padilla 2019, 505). Compréndase que la palabra *deepfake* es de origen anglosajón, y posee la estructura de una palabra compuesta: *deep* significa 'profundo' y *fake*, 'mentira'. Las imágenes de las estudiantes fueron incorporadas en fotografías y videos de connotación sexual/pornográfica, gracias

a herramientas tecnológicas automatizadas (la IA) para crear una mentira (profunda) de alta gravedad.

No obstante, este no es el único fenómeno que se deriva del uso de las nuevas tecnologías y de internet. La globalización se ha convertido en caldo de cultivo para la aparición de nuevos comportamientos o conductas que afectan el libre desarrollo del ser humano, además de reestructurar la concepción tradicional de una sociedad. A partir del año 2011, la Relatoría Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, junto con otros relatores de esa misma rama de protección internacional, promulgaron la Declaración Conjunta sobre Libertad de Expresión e Internet, el primer marco regulatorio internacional sobre la comprensión del acceso a internet como un derecho conexo a la libertad de expresión y, por ende, un derecho humano (Organización de las Naciones Unidas [ONU] et al. 2011). Este fue un primer intento por proteger a las personas en el mundo digital, pero no fue suficiente, considerando las diversas formas de atentar contra los derechos de privacidad o integridad.

Un concepto que define de forma poliédrica los fenómenos negativos que emergieron de la globalización es *violencia digital*. Estas palabras representan con precisión el trasfondo del Caso 700 IA. Por esa razón, resulta importante su comprensión bajo los siguientes términos:

> La violencia digital existe porque existe una violencia que la precede y con la que se retroalimenta, que es la violencia diaria vivida en las calles, colegios, trabajos, plazas, boliches, canchas de fútbol, etc. Es entendible y lógico que la violencia tenga su versión digital. Así como la mayoría de las prácticas comenzaron a digitalizarse, las violencias hicieron lo mismo. (Faro Digital 2019, 3)

La digitalización de la violencia es un fenómeno progresivo en congruencia con el diseño de nuevas tecnologías de la información. Cabe destacar que la mayoría de las tipologías de violencia digital se han concentrado en la esfera de la intimidad y la privacidad sexual de los usuarios de internet; por esa razón, la agenda legislativa o parlamentaria de algunos Estados ha priorizado su regulación. Un claro ejemplo es el avance normativo de Ecuador en el proceso de reforma al Código Orgánico Integral Penal (EC 2021b) para la lucha contra los delitos informáticos. Dentro de este proceso regulatorio, se reformaron bastantes tipos penales para sancionar conductas antijurídicas cometidas a través de medios digitales y combatir la violencia sexual digital; en la reforma se penalizan actividades como el *sexting*,[1] el *grooming*[2] y el *ciberbullying*.[3]

1 "[A]cción de filmarse o sacarse una foto con contenido sexual, erótico o pornográfico y enviar esas imágenes o videos a una persona de confianza por medio del celular u otro dispositivo electrónico" (AR Ministerio de Justicia y Derechos Humanos 2023b, 1).
2 "[A]coso sexual de una persona adulta a una niña, un niño o un adolescente por medio de internet. Las personas que realizan *grooming* se llaman *groomers* o *acosadores*" (AR Ministerio de Justicia y Derechos Humanos 2023a, 1).
3 "Toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico, que de forma directa o indirecta, ejerce un docente, autoridad o aquel con quien la víctima o víctimas mantiene una relación de poder asimétrica que, en forma individual o colectiva, atente en contra de una o varias personas por medio de las tecnologías de la información y comunicación" (EC 2014, art. 154, num. 3).

Un nuevo personaje en la globalización: la inteligencia artificial

En este texto se ha utilizado un enfoque multidisciplinario para la definición y descripción de la IA. El objetivo de este acápite es desarrollar un marco conceptual sobre la IA y sus categorías a partir de sus funciones, para prevenir la desinformación en torno a su alcance o incidencia negativa en las relaciones humanas. Precisamente, en las ciencias jurídicas, muchos abogados y abogadas han tenido la iniciativa equivocada de explicar esta tecnología desde un enfoque técnico; es un error, porque aquel abogado o abogada sin conocimiento especializado en la programación o el diseño de sistemas automatizados tiende a dar una apreciación sesgada por su rama de estudios (ciencias jurídicas), con la consecuente falta de veracidad en sus argumentos y la determinación de una realidad adversa a la que corresponde a una línea de investigación técnica de la IA.

En primer lugar, para resolver esta gran interrogante del siglo XXI, ¿qué es la IA?, es necesario entender la similitud conceptual entre inteligencia y racionalidad. Un sistema es racional si actúa "correctamente" en virtud de sus conocimientos (Russel y Norving 2004). El concepto de IA depende de su acercamiento conceptual; por ejemplo, si se parte desde una visión de la IA como un sistema que actúa igual a un humano, *inteligencia artificial* vendría a ser "[e]l arte de desarrollar máquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren de inteligencia" (Kurzweil 1990, 47-8). Por otro lado, si la perspectiva nace desde la comprensión de la IA como un sistema que actúa racionalmente, se dice que "está relacionada con conductas inteligentes en artefactos" (Nilsson 1998, 53). No obstante, el origen del término *inteligencia artificial* se remonta al año 1956, cuando John McCarthy lo utilizó para hacer referencia a "la ciencia y la ingeniería de crear máquinas inteligentes, especialmente programas de computación inteligentes" (ES Agencia Española de Protección de Datos Personales [AEPD] 2020, 5). Según las definiciones citadas, se puede describir a la IA como un sistema automatizado para proveer respuestas frente a preguntas o requerimientos humanos.

La automatización de procesos no es un factor que se atribuya únicamente a la IA. En realidad, alrededor del año 1500, el científico y pintor Leonardo da Vinci diseñó, sin llegar a construirla, la primera calculadora mecánica, cuyo éxito funcional se demostró años después. Este antecedente guio la construcción de la primera máquina calculadora en el año 1623, por parte del científico alemán Schickard (Russel y Norving 2004). Al describir las funciones de la calculadora, se puede identificar un proceso similar al de la IA. Considérese el siguiente ejemplo: si una persona necesita resolver un problema aritmético y requiere de una solución óptima, que no genere una inversión humana de tiempo para ejecutarlo, ingresará el problema aritmético a la calculadora, y al presionar un botón obtendrá la respuesta de forma automática. Comparando esta actividad con un sistema de IA, cuando un individuo necesite elaborar un ensayo y no quiera emplear su tiempo para ello, ingresará su solicitud a una plataforma de IA y, de forma automática, obtendrá el resultado.

La IA clásica tiene modelos de funcionamiento que se basan en dos premisas (Banda 2014):

1. Representación formal del problema que se busca resolver, como una red semántica.
2. Capacidad de procesamiento simbólico, derivado de algoritmos en búsqueda de soluciones.

De estas premisas emerge un concepto importante para el funcionamiento de la IA: computación simbólica, que hace alusión a "la solución algorítmica de problemas relacionados con objetos simbólicos. Se consideran objetos simbólicos todos los objetos matemáticos y sus representaciones computacionales; por ejemplo, aquellos que corresponden al álgebra computacional y a la lógica computacional" (Banda 2014, 49).

La IA clásica tiene tres métodos para ofrecer soluciones algorítmicas frente a problemas o requerimientos humanos: 1. simulación cognitiva, 2. sistemas basados en lógica y 3. sistemas basados en conocimiento. El primero se fundamenta en la hipótesis de que el procesador cognitivo escoge preceptos y reacciona ante ellos en ciclos de reconocimiento y acción, en unos 70 milisegundos, mientras que las transferencias entre la memoria a corto plazo y la memoria a largo plazo tardarían unos siete segundos. El segundo método establece que la lógica es el elemento esencial de la IA para la representación del conocimiento y del razonamiento. El tercero, finalmente, se sustenta en la captura, codificación y utilización del conocimiento de expertos humanos (Banda 2014).

Adentrándose en el mundo del tratamiento de datos personales, la IA ha adquirido un rol trascendental. En esta dimensión también se desprenden cinco categorías de la IA, según su función en el procesamiento de datos (ES AEPD 2020):

1. Entrenamiento: La IA en entrenamiento es, prácticamente, una técnica de *machine learning*. Esta técnica y su relación con la IA se puede entender en las siguientes palabras:

> El *machine learning* diseña modelos predictivos que construyen por sí mismos la relación entre las variables a estudiar mediante el análisis de un conjunto inicial de datos, la identificación de patrones y el establecimiento de criterios de clasificación. Una vez fijados los criterios, al introducir un nuevo conjunto de datos el componente IA es capaz de realizar una inferencia. (ES AEPD 2020, 12)

2. Validación: En esta categoría se busca identificar la bondad del modelo utilizado en el tratamiento de datos personales.
3. Despliegue: La solución del sistema de IA se obtiene a través de la comunicación de datos personales a terceros.
4. Explotación: En esta categoría existen subclasificaciones que se dividen por la solución del sistema IA y su tratamiento de datos personales:

a. Inferencia: Cuando se utilizan datos de una persona para obtener un resultado, se utilizan datos de terceros con el mismo propósito, o cuando los datos e inferencias de la persona se almacenan en el sistema de IA.
b. Decisión: Cuando la solución del sistema de IA decide sobre los datos de la persona.
c. Evolución: Cuando la solución del sistema de IA utiliza datos personales de quien realizó la consulta o los resultados obtenidos, con el objetivo de seguir mejorando y depurarse.

5. Retirada: Cuando un servicio de un sistema de IA se retira del mercado o un usuario decide no continuar con él.

En conclusión, para terminar este acápite basta con haber comprendido a la IA desde su enfoque multidisciplinario. La descripción profunda sobre la dimensión técnica de la IA no garantiza su entendimiento humano; resulta más didáctico estudiar sus características inherentes, funciones y antecedentes. La definición de la IA a partir de su clasificación en virtud de los tratamientos de datos, o de su metodología para resolver una inquietud humana, ejemplifica de forma pragmática su utilización.

Protección de datos personales

Breve radiografía internacional de la protección de datos personales

En el año 2017 se transformó la cosmovisión empresarial y legal con la adopción de una nueva premisa global: "El recurso más valioso del mundo ya no es el petróleo, sino los datos". Este es el título de un artículo de la revista *The Economist* (2017) en el que se describe la importancia de los datos en el fenómeno de la globalización y las nuevas tecnologías; incluso, incentiva la elaboración de políticas antimonopolio para evitar un tratamiento agresivo, ilegítimo o ilícito de datos personales de los consumidores. Para ejemplificar esta cosmovisión, un ejemplo claro es el perfilamiento de datos personales, a través de redes sociales, para la segmentación de mercado y programación de estrategias de *marketing* personalizadas con el objetivo de persuadir al consumidor de que compre un producto o contrate un servicio de una empresa sobre otra.

El Parlamento de la Unión Europea, un año antes de esta publicación, promulgó el Reglamento General de Protección de Datos (RGPD), con lo que afianzó su consciencia regulatoria relativa al tratamiento de datos como mecanismo estratégico para la economía de las corporaciones tecnológicas. El RGPD se convirtió en el primer marco normativo comunitario en prescribir las obligaciones derivadas del derecho a la protección de datos de personales; presentó un catálogo extenso de conceptos inusuales para el mundo del derecho, que merecen su atención para la comprensión del Caso 700 IA.

El primer término a comprender es *dato personal*, que según el RGPD es

> toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (Parlamento de la Unión Europea y Consejo de la Unión Europea 2016, art. 4)

La segunda palabra es *tratamiento*, que se encuentra definida por el RGPD en los siguientes términos:

> [C]ualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. (art. 4)

Dentro de este concepto cabe la manipulación de las imágenes de las estudiantes víctimas de la creación de contenido sexual en el Caso 700 IA.

Ahora bien, el régimen de protección de datos está compuesto por roles específicos, con sus respectivas obligaciones y sanciones. El primero se denomina "responsable del tratamiento de datos personales": "[P]ersona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" (art. 4). El segundo rol es el "encargado de tratamiento de datos personales", conceptualizado en los siguientes términos: "[P]ersona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento" (art. 4). Cabe mencionar que en el marco comunitario europeo se prevén roles adicionales; sin embargo, estos serán los desarrollados a la luz del marco normativo ecuatoriano.

El RGPD promueve un sistema de protección de datos personales para cada uno de los Estados miembros de la Unión Europea. En el transcurso de siete años, aproximadamente, se han conocido sanciones económicas exorbitantes a múltiples corporaciones que lideran el mercado global, lo que marca un precedente constante frente a la importancia de precautelar el derecho a la protección de datos personales y la privacidad.

En la búsqueda de una interpretación teleológica sobre el régimen comunitario de protección de datos personales, se puede detectar que el RGPD fue creado no solo para proteger los datos de los y las ciudadanas de los Estados miembros de la Unión Europea, sino también para prevenir la visión empresarial agresiva en la analítica de datos, que puede provocar actos de competencia desleal en el mercado mundial. No sería correcto ocultar la realidad del "Corporate America", cuyo fundamento ideológico consistía en el postulado "*It is a government of corporations, by corporations, for corporations*", y que de-

mandó la ejecución de prácticas más éticas para el sector empresarial a nivel global (Saad 2020). Desde esa perspectiva, la actuación de la mayoría de las autoridades de control en materia de protección de datos, dentro de la Unión Europea, está dirigida hacia las empresas como responsables del tratamiento de datos personales; por esa razón, no existen muchas sanciones a personas naturales que actúan como responsables del tratamiento.

En el régimen de protección de datos del RGPD se establecen bases de legitimación para el tratamiento de datos personales. Compréndanse como *base de legitimación* aquellos supuestos en los que el tratamiento de datos es lícito, legítimo y, por ende, no susceptibles de una sanción. Los supuestos para la legitimación del tratamiento son:

1. El consentimiento del titular de los datos personales.
2. Si el tratamiento es necesario para el cumplimiento de un contrato.
3. Si el tratamiento es necesario para el cumplimiento de una obligación legal.
4. Si el tratamiento es necesario para proteger y precautelar el interés vital del titular de los datos o de otra persona natural.
5. Si el tratamiento es necesario para el cumplimiento de una misión de interés público.
6. Si existe un interés legítimo para el tratamiento de datos.
7. Si el tratamiento de datos proviene de una fuente pública de información. (Parlamento de la Unión Europea y Consejo de la Unión Europea 2016, art. 6)

Resultaba importante describir los roles del régimen de protección de datos personales y las bases de legitimación según el RGPD, debido a que es el marco regulatorio más influyente en los cuerpos normativos en materia de protección de datos personales en América Latina. Asimismo, su interpretación teleológica permite identificar la cosmovisión de una autoridad de control y el sistema de protección de datos personales.

Protección de datos personales en Ecuador

El 26 de mayo de 2021 se publicó en la gaceta del Registro Oficial de Ecuador la Ley Orgánica de Protección de Datos Personales (EC 2021a). De forma concreta, el proceso regulatorio se caracterizó por utilizar, prácticamente, la estructura de forma y fondo del RGPD. No obstante, es importante resaltar la preexistencia del derecho constitucional a la protección de datos personales en el art. 66, num. 19, de la Constitución (EC 2008):

> Se reconoce y garantizará a las personas [...] [e]l derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley.

En esta descripción se pueden observar diferentes conceptos, como el de tratamiento de datos personales y el de titular de los datos personales. Adicionalmente, el artículo prescribe con bastante precisión el ciclo de vida de los datos personales:

Figura 1. Ciclo de vida de los datos personales.
Elaboración propia a partir de EC (2008, art. 66, num. 19).

El ciclo de vida inicia con la captura de datos personales para después almacenarlos en repositorios físicos o digitales. Una vez almacenada la información, se realiza el procesamiento de los datos; por ejemplo, perfilamiento o analítica de datos. En algunos casos, se los transfiere o comunica a terceros externos. La última fase es la eliminación de la información.

Otra institución jurídica que contribuyó al desarrollo normativo de la protección de datos personales es el *habeas data*. La Corte Constitucional del Ecuador (2015, 14) la ha definido como la

> garantía constitucional que le permite a la persona natural o jurídica acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado, a fin de conocer el contenido de la misma y, de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causa algún tipo de perjuicio a efectos de salvaguardar su derecho a la intimidad personal y familiar.

Este concepto promovió la normativización de los derechos de acceso, rectificación, cancelación y oposición a la información, más conocidos como "derechos ARCO Plus". Es interesante que la institución del *habeas data* como elemento precursor de la Ley Orgánica de Protección de Datos Personales haya aparecido por primera vez en el ordenamiento jurídico ecuatoriano en el año 1979 en Ecuador (Guerrero 2020); este detalle histórico demuestra cuánto tardaron la Función Legislativa y la voluntad política frente a la regulación de la protección de datos personales.

Enfocándose en la ley, se puede descubrir un catálogo más amplio de conceptos que conforman el régimen de protección de datos personales. Para comenzar, el cuerpo normativo prevé una categoría más extensa de datos personales, en los que se destacan los datos sensibles, definidos como

> [d]atos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. (EC 2021a, art. 4)

Además, se describe una estructura pormenorizada de los partícipes en el sistema de protección de datos:

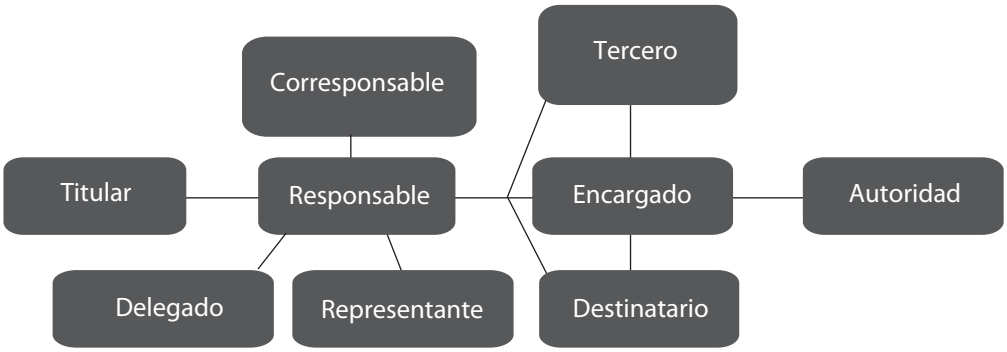

Figura 2. Sistema de protección de datos personales en Ecuador.
Elaboración propia a partir de EC (2021a, art. 4).

Según la ley, el titular es la "[p]ersona natural cuyos datos son objeto de tratamiento" (art. 4). El rol de corresponsable está previsto en el RGPD de la siguiente manera: "Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento" (Parlamento de la Unión Europea y Consejo de la Unión Europea 2016, art. 4).

El rol de delegado de protección de datos personales es muy similar al del oficial de cumplimiento. La diferencia radica en las materias a las que se dedican uno y otro. Según la Ley Orgánica de Protección de Datos Personales, el delegado es la

> [p]ersona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos. (EC 2021a, art. 4)

Por otro lado, el oficial de cumplimiento está definido en los siguientes términos:

> [P]ersona natural idónea y calificada, que tiene la responsabilidad de vigilar la adecuada implementación y funcionamiento del Sistema de Prevención de Riesgos, siendo asimismo responsable de velar por la implementación y observancia de las políticas, controles y procedimientos necesarios para la prevención de lavado de activos, financiamiento del terrorismo y otros delitos, y de verificar la aplicación de la normativa existente sobre la materia. (EC Superintendencia de Compañías, Valores y Seguros 2023, art. 3)

La definición de *destinatario* está en la ley y en el RGPD, pero para este estudio se ha optado por utilizar lo que prescribe el cuerpo normativo ecuatoriano: "Persona natural o jurídica que ha sido comunicada con datos personales" (EC 2021a, art. 4).

Sobre el rol del representante y del tercero, ambos fueron desarrollados en el reciente reglamento a la ley:

> 1. Tercero.– Persona natural o jurídica, autoridad, servicio u organismo distinto al titular, del responsable del tratamiento, del encargado del tratamiento, y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable.
>
> 2. Representante.– Persona natural o jurídica establecida en el territorio ecuatoriano que, habiendo sido designada por escrito por el Responsable o el Encargado del tratamiento de datos, les represente en lo que respecta a sus obligaciones según la Ley. (EC 2023, art. 4)

Finalmente, a inicios del año 2024, en Ecuador aún persiste la ausencia de la autoridad de protección de datos personales. El Consejo de Participación Ciudadana y Control Social tiene la obligación y responsabilidad de seleccionar al o a la superintendenta por medio de un proceso transparente y meritocrático, atendiendo a los requisitos de perfil previstos por la normativa correspondiente. Esto quiere decir que el sistema de protección de datos personales no se ha completado en su totalidad por la ausencia de su actor sancionador, lo que provoca la falta de tutela idónea del derecho a la protección de datos personales.

Análisis del Caso 700 IA

En este acápite se realizará un ejercicio de concatenación y subsunción de los hechos al marco normativo aplicable, además de identificar la actuación de la IA dentro de los principios de regulación estandarizados por la Unión Europea y el régimen de protección de datos europeo y ecuatoriano.

En primer lugar, es menester definir si las imágenes manipuladas para la creación de archivos de contenido sexual son datos personales, y si pertenecen a una categoría de datos personales. La Ley Orgánica de Protección de Datos Personales define a un dato personal como aquella información que hace identificable a un ser humano. Asimismo, la Corte Constitucional del Ecuador (2021) ha reconocido a las imágenes fotográficas como un dato personal que pertenece a la categoría de datos sensibles, y que exige una protección reforzada. Es interesante que el primer precedente en materia de protección de datos personales fue la interpretación de la Corte Constitucional en un caso que trataba sobre *sexting* dentro de un colegio, es decir, el mismo contexto fáctico del Caso 700 IA.

Cabe destacar que, en el derecho comparado, la AEPD ha sancionado a una persona natural y su empresa, dentro de la misma causa, por el tratamiento de imágenes obtenidas de la red social de una modelo sin su consentimiento. El factor diferencial de este caso es que las imágenes solo mostraban las piernas de la persona (ES AEPD 2023). Este es un claro ejemplo de la concepción de las imágenes como datos personales susceptibles de protección bajo un régimen normativo específico en dicha materia.

Adicionalmente, en el Caso 700 IA, las imágenes pertenecían a menores de edad; entonces, poseen la categoría especial de datos personales de menores de edad, previsto en el art. 25 de la Ley Orgánica de Protección de Datos Personales, de modo que están revestidos de una protección reforzada (EC 2021a). Por todo lo expuesto, la precautela hacia las imágenes de las estudiantes tienen una doble protección reforzada, por pertenecer a la categoría de datos sensibles y de menores de edad.

Ahora bien, es menester identificar a los involucrados dentro del Caso 700 IA y qué rol les corresponde según el sistema de protección de datos personales ecuatoriano. Los involucrados son:

1. Jóvenes estudiantes que manipularon las imágenes de sus compañeras, a los que se denominará "sujetos A".
2. Las compañeras estudiantes que fueron víctimas de la manipulación de sus imágenes, a las que se denominará "sujetos B".

Los sujetos A adquieren el rol de responsables del tratamiento de datos personales al manipular las imágenes de los sujetos B, que actúan como titulares de dicha información. Son responsables porque definieron la finalidad del tratamiento sobre las imágenes: en este caso, la creación de archivos de contenido sexual.

Resulta pertinente identificar si existe alguna base de legitimación para que los sujetos A hayan tratado lícitamente los datos personales de los sujetos B. En este punto se forma la singularidad que provocó la afectación hacia el derecho a la protección de datos personales de los sujetos B, debido a que la creación de contenido sexual con menores de edad es en sí mismo un tratamiento de datos ilícito. En el acápite introductorio de este texto se citaban las reformas al Código Orgánico Integral Penal del Ecuador para luchar contra la violencia digital y los delitos informáticos. En ese cuerpo normativo se modificó el artículo que penalizaba la pornografía infantil, para prescribirlo de la siguiente forma:

> Pornografía con utilización de niñas, niños o adolescentes.– La persona que fotografíe, filme, grabe, produzca, transmita o *edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual*, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. (EC 2021b, art. 103; énfasis añadido)

Dado que el tratamiento, desde su naturaleza, es una actividad ilícita penalizada, se permitió a los sujetos B tutelar su derecho a la protección de datos personales en el derecho penal. De esta forma, el sistema de protección de datos personales ecuatoriano fue invisibilizado para actuar dentro del Caso 700 IA. Lamentablemente, si los sujetos B hubieran tratado de tutelar su derecho a la protección de datos en el sistema de protección de datos que prevé la ley, tampoco habría sido posible, porque no existe aún una autoridad que pueda recibir la denuncia o el reclamo. Por esta razón, el Caso 700 IA se está resolviendo en una sede jurisdiccional con un enfoque estrictamente del derecho penal, lo que impide el desarrollo interpretativo a la Ley Orgánica de Protección de Datos Personales y el uso de la IA para el tratamiento de datos personales. Sin embargo, a efectos didácticos y académicos, se realizará un estudio sobre la protección de datos personales y el uso de la IA según el marco fáctico del Caso 700 IA.

La Comisión Europea, órgano ejecutivo de la Unión Europea, está en el proceso de regulación de la IA. Durante su investigación regulatoria, determinó a la ética digital como elemento esencial de un proyecto de ley que normativice la IA. Este elemento será alcanzado siempre y cuando se cumplan los siguientes requisitos: "[A]cción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas" (ES AEPD 2020, 7).

La AEPD ha avanzado en el desarrollo sobre la comprensión del tratamiento de datos personales por medio de herramientas, sistemas o plataformas de IA. El aporte más importante es la relación entre los roles que prevé el RGPD —muy similares a los de la Ley Orgánica de Protección de Datos Personales— y las categorías de sistemas de IA según su funcionamiento, que fueron descritos con anterioridad: 1. entrenamiento, 2. validación, 3. despliegue, y 4. explotación y sus subclasificaciones (12-3). El siguiente esquema puede simplificar lo mencionado:

Tabla 1
Esquema sobre la relación entre los roles del sistema de protección de datos personales y el uso de la inteligencia artificial

Función de la IA	Responsable del tratamiento de datos personales	Encargado del tratamiento de datos personales
Entrenamiento	Será responsable del tratamiento de datos personales aquella empresa o persona física que utilice datos personales para entrenar al sistema de IA.	Será encargado del tratamiento de datos personales aquella empresa o persona física contratada por el responsable para que realice tratamientos designados por este mismo, cuyo objetivo principal será el entrenamiento del sistema de IA.
Validación	Es igual que el caso anterior, solo cambia la función que realizará el sistema de IA.	Es igual que el caso anterior, solo cambia la función que realizará el sistema de IA.
Despliegue	Será responsable del tratamiento de datos personales aquella empresa o persona física que comunique los datos personales a otra entidad, empresa o persona natural para que realice un tratamiento autónomo e independiente, lo que la convertirá en corresponsable del tratamiento.	Será encargado del tratamiento de datos personales aquella empresa o persona física que preste un servicio con sistema de IA de comunicación de datos personales al responsable, siempre y cuando solo este pueda tratarlos.
Explotación: inferencia	Será responsable del tratamiento de datos personales aquella empresa o persona física que trate los datos personales para sus propios fines por medio del uso general de sistemas de IA.	Es igual que el caso anterior, solo varía la función del sistema de IA.
Explotación: decisión	Será responsable del tratamiento de datos personales aquella empresa o persona física que tome decisiones automatizadas sobre los datos de su titular, por medio del uso de un sistema de IA.	Es igual que el caso anterior, solo varía la función del sistema de IA.
Explotación: evolución	Será responsable del tratamiento de datos personales aquella empresa o persona física que determine la evolución del sistema de IA tras el tratamiento de datos personales de los usuarios de dicho sistema.	Será encargado del tratamiento de datos personales aquella empresa o persona física que contrate a una entidad, empresa o persona para que realice un tratamiento de datos con un sistema de IA.

Elaboración propia a partir de ES AEPD (2020).

En conclusión, será un desafío para el derecho procesal penal dentro del Caso 700 IA considerar los elementos de fondo, como la protección de datos personales y el uso de la IA. Es cuestionable el alcance interpretativo de este caso, debido al límite por su materia de jurisdicción y la terrible ausencia de la autoridad en protección de datos personales. No es inaudito pensar en la posibilidad de que, en algún momento, la autoridad pueda avocar conocimiento sobre este caso y realizar una interpretación favorable para la idoneidad de la aplicación del sistema de protección de datos personales ecuatoriano.

Referencias

AR Ministerio de Justicia y Derechos Humanos. 2023a. *Grooming: Guía práctica para adultos.* Buenos Aires: Ministerio de Justicia y Derechos Humanos.

—. 2023b. *Sexting: Guía práctica para adultos.* Buenos Aires: Ministerio de Justicia y Derechos Humanos.

Banda, Hugo. 2014. *Inteligencia artificial: Principios y aplicaciones*. Quito: Escuela Politécnica Nacional del Ecuador.

Cerdán, Víctor, y Graciela Padilla. 2019. "Historia del fake audiovisual: Deepfake y la mujer en un imaginario". *Historia y Comunicación Social* 24 (2): 505-20. https://tinyurl.com/bdd4rz59.

EC. 2008. *Constitución de la República del Ecuador*. Registro Oficial 449, 20 de octubre.

—. 2014. *Código Orgánico Integral Penal*. Registro Oficial 180, Suplemento, 10 de febrero.

—. 2021a. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial 459, 26 de mayo.

—. 2021b. *Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos*. Registro Oficial 526, 30 de agosto.

—. 2023. *Reglamento a la Ley Orgánica de Protección de Datos Personales.* Registro Oficial 435, Suplemento, 11 de noviembre.

EC Corte Constitucional. 2015. "Sentencia n.° 182-15-SEP-CC". En *Caso n.° 1493-10-EP*. 3 de junio.

—. 2021. "Sentencia". En *Caso n.° 2064-14-EP*. 27 de enero.

EC Superintendencia de Compañías, Valores y Seguros. 2023. *Normas para control del lavado de activos en el sector societario.* Registro Oficial 248, 10 de febrero.

El Universo. 2023. "Un caso de violencia sexual usando inteligencia artificial se reporta en un colegio, en Quito". *El Universo*. 4 de octubre. https://tinyurl.com/25uuwakn

ES AEPD. 2020. *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial: Una introducción*. Madrid: AEPD,

—. 2023. *Expediente n.° EXP202207521*. 5 de julio.

Faro Digital. 2019. *Perspectivas: Informe sobre violencia digital.* Buenos Aires: Faro Digital. https://tinyurl.com/5c82cuva.

Guerrero, Juan Francisco. 2020. *Las garantías jurisdiccionales constitucionales en el Ecuador.* Quito: Corporación de Estudios y Publicaciones.

Kurzweil, Raymond. 1990. *The Age of Intelligent Machines.* Boston: MIT Press.

Loaiza, Yalilé. 2023. "Estudiantes de un colegio de Quito utilizaron fotografías de sus compañeras para crear contenido sexual con inteligencia artificial". *Infobae*. 5 de octubre. https://tinyurl.com/2efz8p9w.

Nilsson, Nils. 1998. *Artificial Intelligence: A New Synthesis.* San Francisco, US: Morgan Kauffman.

ONU, Organización para la Seguridad y la Cooperación en Europa, Organización de Estados Americanos (OEA) y Comisión Africana de Derechos Humanos y de los Pueblos. 2011. Declaración conjunta sobre libertad de expresión e internet. *OEA*. 1 de junio. https://tinyurl.com/5n8nht3e.

Parlamento de la Unión Europea, y Consejo de la Unión Europea. 2016. *Reglamento General de Protección de Datos*. Diario Oficial de la Unión Europea L119/1. 27 de abril. https://tinyurl.com/3vfyj2ew.

Russel, Stuart, y Peter Norving. 2004. *Inteligencia artificial: Un enfoque moderno.* Madrid: Pearson.

Saad, Eduardo. 2020. *Ética en los negocios y "compliance"*. Buenos Aires: Hammurabi.

The Economist. 2017. "The World's Most Valuable Resource Is No Longer Oil, but Data". *The Economist.* 6 de mayo. https://tinyurl.com/bd2sdeyr.

Declaración de autoría

Daniel Fernando Mejía Terán participó en la conceptualización, investigación, aplicación metodológica, redacción del borrador y edición final.

Declaración de conflicto de intereses

El autor declara no tener ningún conflicto de interés financiero, académico ni personal que pueda haber influido en la realización del estudio.