

# DATA PROTECTION AND PRIVACY THEMATIC AREA NARRATIVE IN ENGLISH ARABIC FRENCH PORTUGUESE AND SPANISH

Rachel Adams , Kelly Stone

Rachel Adams , Kelly Stone

©2025, RACHEL ADAMS , KELLY STONE



This work is licensed under the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/legalcode>), which permits unrestricted use, distribution, and reproduction, provided the original work is properly credited. Cette œuvre est mise à disposition selon les termes de la licence Creative Commons Attribution (<https://creativecommons.org/licenses/by/4.0/legalcode>), qui permet l'utilisation, la distribution et la reproduction sans restriction, pourvu que le mérite de la création originale soit adéquatement reconnu.

*IDRC GRANT / SUBVENTION DU CRDI : - GLOBAL INDEX ON RESPONSIBLE ARTIFICIAL INTELLIGENCE*

# Índice Global sobre IA Responsable

Dimensión: Derechos humanos e IA

Subdimensión: Derechos civiles y políticos

Área temática: [Privacidad, intimidad y protección de datos](#)

## Definiciones

El [derecho a la intimidad](#) se define como el derecho de una persona "a no sufrir intromisiones o divulgación de asuntos de carácter personal"<sup>1</sup> por parte del gobierno y/o de terceros, ya sean entidades privadas o particulares. Aunque el derecho a la intimidad ha sido consagrado en diversos marcos jurídicos, su primera referencia como **derecho humano** apenas se produjo en 1948, cuando la Asamblea General de las Naciones Unidas adoptó el [artículo 12](#) de la Declaración Universal de los Derechos Humanos (DUDH), antes de ser inscrito como derecho individual en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos ([PIDCP](#)). Cabe destacar que el derecho a la intimidad no es un [derecho absoluto](#) y puede limitarse por las circunstancias previstas por la ley, como la protección de intereses de seguridad nacional o en la prevención y persecución de casos penales.

El derecho a la privacidad ha evolucionado, incluyendo ahora la [privacidad de información](#), que se define como el derecho de una persona a tener el control sobre quién tiene acceso a sus **datos personales** y con qué fines. Los [Principios de la UNESCO sobre la protección de los datos personales y la privacidad](#) definen los datos personales como "toda información relativa a una persona (interesado) que permite identificarla directa o indirectamente", ya sea por referencia a esos datos o mediante "medidas de una probabilidad razonable" llevadas a cabo por herramientas y sistemas de IA.

Por lo tanto, el derecho a la intimidad, en particular a la privacidad de la información, la **protección de datos** y el **tratamiento de los mismos** está estrechamente relacionado. La **protección de datos** es una de las formas de proteger el derecho a la intimidad, a través de la [regulación del tratamiento](#) de datos y de la información personal, y del establecimiento de mecanismos de responsabilización, en caso de uso indebido de datos personales. El [tratamiento de datos](#) se define como "la serie de operaciones manuales, automáticas o electrónicas como validación, clasificación, reducción y agregación de datos".<sup>2</sup> "Estas operaciones suelen ir seguidas de la extracción, transformación, clasificación, análisis y presentación de datos".<sup>3</sup>

## Justificaciones

Los marcos normativos internacionales en materia de IA han destacado la importancia de la relación entre el derecho a la intimidad y la protección de datos. En particular, los

<sup>1</sup> Traducción no oficial

<sup>2</sup> Traducción no oficial

<sup>3</sup> Traducción no oficial

[Principios de la OCDE sobre IA](#) apelan a que los agentes de la IA garanticen medidas de protección de datos y la Recomendación de la UNESCO sobre la Ética de la IA (Recomendación) aboga por que el tratamiento de los datos personales se realice con base en la ley. Además, los [Principios de la UNESCO sobre la protección de los datos personales y la privacidad](#) establecen una lista de diez principios para la protección de datos, sobre: tratamiento justo y lícito; especificación de la finalidad, la proporcionalidad y la necesidad; la limitación de la conservación de los datos; la exactitud; la confidencialidad; la seguridad; la transparencia; las transferencias; y la responsabilidad. Y es que la legislación sobre protección de datos se configura como la piedra angular de una IA responsable.

A pesar de los diversos principios internacionales que defienden la importancia del derecho a la intimidad y la protección de datos, el desarrollo y uso de sistemas de IA implica, con frecuencia, el tratamiento de información personal sensible, aumentando así el riesgo de [vulnerar](#) el derecho a la intimidad. Durante la fase de formación, los algoritmos, los asistentes de voz y los mecanismos de recomendación recopilan, integran y analizan grandes conjuntos de datos, tomando luego [decisiones](#) en tiempo real. Los datos personales o sensibles pueden ser introducidos directamente por el usuario o capturados de forma más encubierta, a través del uso de cookies y de otros mecanismos de rastreo. Son luego procesados para predecir [pautas](#) de consumo, lo cual, si no se regula de forma adecuada, amenaza el derecho de los usuarios a la intimidad y otros derechos relacionados.

Por consiguiente, la evaluación de este tema resulta esencial para analizar la IA de forma responsable. Las consideraciones sobre la protección de datos en la IA incluyen la garantía de que la recopilación, el tratamiento y almacenamiento de datos personales se realiza de forma lícita; el establecimiento de medidas de seguridad adecuadas para proteger los datos personales; el control y una auditoría sistemática de la utilización de los datos personales para garantizar su uso lícito y legítimo; y el proporcionar a los usuarios "[información clara y transparente](#)" sobre el uso de sus datos personales, incluidos sus derechos en relación con el tratamiento de los referidos datos.

## Identificaciones

Esta área temática examina las medidas adoptadas por los países para proteger el derecho a la intimidad y a la protección de datos en el diseño, desarrollo y uso de herramientas y sistemas de IA. En concreto, el análisis debe tener en cuenta (1) los **marcos jurídicos** relativos a los sistemas de IA, (2) las **acciones gubernamentales** para aplicar estos marcos o abordar cuestiones relacionadas con la protección y la privacidad de los datos, y (3) los **agentes no estatales** que trabajan en la protección de la privacidad y de los datos, en el país en cuestión.

**Los marcos jurídicos** del país pueden adoptar la forma de leyes, reglamentos, políticas (incluso por sector y/o departamento) y/o directrices. Las **acciones gubernamentales** pueden incluir la elaboración de proyectos de ley o políticas relacionadas con la protección de datos y la privacidad en la IA, la creación de grupos de trabajo gubernamentales u organismos de supervisión encargados de ofrecer recomendaciones políticas o de supervisar el cumplimiento de la legislación sobre protección de datos en el despliegue de los sistemas de IA. Los **Agentes No Estatales (ANE)** pueden ser organizaciones no gubernamentales (ONG), pero también empresas multinacionales,

organizaciones militares privadas, medios de comunicación, grupos étnicos organizados, instituciones académicas, grupos de presión, sindicatos o movimientos sociales que trabajan para reforzar los protocolos relativos a la protección de datos y a la intimidad en el contexto de la IA.

## Ejemplos:

### *Marcos jurídicos*

En el Reino Unido, la Ley de Protección de Datos de 2018 ([DPA 2018](#)), junto con la [adaptación específica](#) para el Reino Unido del Reglamento General de Protección de Datos ([RGPD](#)) de la Unión Europea, establece definiciones esenciales, principios de protección de datos y base jurídica para el tratamiento de datos, así como requisitos de responsabilidad para organizaciones e individuos involucrados en el tratamiento de datos personales, con restricciones más específicas en la Ley. En concreto, la ley establece principios de protección de datos que exigen que estos sean exactos y actualizados, y que su uso sea justo, lícito y transparente, para "fines especificados y explícitos", de forma "adecuada, pertinente", segura y para fines limitados, y que se ofrezca una protección más sólida para la "información más sensible", incluida la relativa a raza, etnia, creencias religiosas, datos biométricos, salud y orientación sexual.

### *Acciones gubernamentales*

El artículo 115 de la Ley de Protección de Datos del Reino Unido (DPA 2018) y el artículo 51 del Reglamento General de Protección de Datos (GDPR) vigente en la Unión Europea contienen las funciones y poderes de ejecución del Information Commissioner's Office (ICO), al que se atribuyen responsabilidades específicas en la regulación de los derechos de datos de las personas. En 2018, el ICO publicó su [Política de Acción Reguladora](#), reiterando sus poderes específicos y delineando su enfoque específico en la ejecución de sus funciones. En 2019, el ICO también lanzó su [Regulatory Sandbox](#), que proporciona servicios gratuitos a las organizaciones que usan datos personales "de forma innovadora y segura"<sup>4</sup> para ayudar a prevenir y atenuar las vulneraciones del derecho a la intimidad y los riesgos de protección de datos, en concreto mediante la integración de la protección de datos en el diseño y desarrollo de los sistemas y herramientas de IA.

### *Agentes no estatales*

En Kenia, la organización [Paradigm Initiative](#) propone soluciones políticas; en concreto, [una de ellas](#) recomienda medidas gubernamentales para la protección de datos, analizando también los marcos jurídicos y políticos, relativos a las Tecnologías de Información y Comunicación (TIC) de toda África, para garantizar la protección de los derechos digitales de los ciudadanos. Proporciona también formación a organizaciones sin ánimo de lucro y establecimientos de enseñanza "sobre el uso de las TIC y la seguridad digital, la defensa de los medios de comunicación social, etc."<sup>5</sup> habiendo creado el Programa de Derechos Digitales a fin de "reforzar las capacidades de las organizaciones de la sociedad civil africana, de los periodistas, de los defensores y de otros, para comprender, defender y promover los derechos digitales".<sup>6</sup> La organización Privacy International, con sede en Londres, publicó una [guía](#) sobre la protección de datos, que puede ser aplicado a las tecnologías de IA.

---

<sup>4</sup> Traducción no oficial

<sup>5</sup> Traducción no oficial

<sup>6</sup> Traducción no oficial

