Homework 4: Information Security

Computer Security

Universidad San Francisco de Quito

Xavier Sebastián Tandazo Cobo

2025

1 Foundational Research: Ecuadorian Data Sovereignty (LOPDP)

1.1 What are the three core principles that govern all data processing activities under the LOPDP?

En el artículo, los tres principios fundamentales que gobiernan todas las actividades de tratamiento de datos personales son los siguientes:

1.1.1 Principio de juridicidad.

De acuerdo con el Artículo 10, en el literal (a), todos los datos personales deben ser tratados bajo un estricto apego a la Constitución de la República del Ecuador, a instrumentos internacionales ratificados por el Estado, a la ley, a su Reglamento y a la demás normativa aplicable.

Este principio exige que todo tratamiento de los datos personales, incluidos los sistemas automatizados y, por consiguiente, basados en IA, cuenten con una base jurídica que sea válida, como el consentimiento de los titulares, una obligación legal o un interés legítimo.

Desde la perspectiva de la seguridad de la información, este principio impone la incorporación de mecanismos de cumplimiento normativo desde el diseño de los sistemas.

1.1.2 Principio de necesidad.

El principio de proporcionalidad y necesidad es reconocido como uno de los criterios mínimos en el Artículo 2, en los literales (e) y (f), y se desarrolla en el Artículo 10, en los literales (e) y (f).

En este principio se establece que los datos personales deben ser pertinentes, adecuados, estrictamente necesarios y no deben ser excesivos en relación con la finalidad perseguida.

En sistemas informáticos y automatizados, este principio obliga a aplicar prácticas de minimización de datos, reduciendo la superficie de ataque y mitigando los riesgos asociados a eventuales vulneraciones de seguridad.

1.1.3 Principio de finalidad.

El Artículo 10, en el literal (d), se consagra el principio de finalidad, conforme al cual los datos personales tienen que ser recolectados para fines determinados, explícitos y legítimos, es decir, que no pueden ser tratados posteriormente para finalidades incompatibles con aquellas para las que fueron inicialmente obtenidos.

En este principio resulta esencial el control de sistemas de decisión automatizada, debido a que limita un uso secundario que no fue autorizado de la información.

Desde el enfoque de seguridad de la información, se exige la implementación de controles de acceso, segmentación de bases de datos y mecanismos de auditoría que garanticen el uso adecuado de los datos personales.

1.2 Locate the specific article (or section within an article) of the LOPDP that grants the data subject the right "to not be object of a decision based solely on automated valuations". Explain the details and protections it provides.

El derecho de los titulares de datos personales a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas se encuentra en el **Artículo 20**, en el Capítulo III relativo a los derechos de los titulares.

Este artículo establece que:

> Cada titular tiene derecho a no ser sometido a una decisión basada *única o parcialmente* en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, cuando dichas decisiones produzcan efectos jurídicos o atenten contra sus derechos y libertades fundamentales

Este derecho resulta útil frente al uso de algoritmos o sistemas de inteligencia artificial que influyen de manera significativa en la situación jurídica o personal del individuo. La norma no solo reconoce el derecho en abstracto, pues además, establece un conjunto de *garantías* para el titular de los datos personales:

- Solicitar al responsable una explicación motivada sobre la decisión adoptada.
- Presentar observaciones respecto a la decisión automatizada.
- Solicitar información sobre los criterios de valoración que fueron utilizados por el sistema.
- Requerir información sobre los tipos de datos que serán empleados y la fuente de su obtención.
- Impugnar la decisión ante el responsable o encargado del tratamiento de datos personales.

El Artículo 20 también delimita las *excepciones* en las que este derecho no puede resultar aplicable, como porejemplo, cuando la decisión automatizada sea necesaria para la celebración o ejecución de un contrato, esté autorizada por una norma jurídica u orden judicial, se base en el consentimiento explícito del titular o no conlleve impactos graves o riesgos verificables para este.

La LOPDP busca reforzar la protección del titular al prohibir expresamente la renuncia anticipada a este derecho por medio de contratos de adhesión y al imponer la obligación de ser informados de forma explícita, a más tardar en la primera comunicación, cuando se trate de decisiones basadas valoraciones automatizadas; el Artículo 20 configura un marco de protección frente a la toma de decisiones automatizadas sin la intervención humana suficiente.

1.3 In the context of an AI-driven system used for decision-making in areas such as hiring processes or loan approvals, Article 20 of Ecuador's Ley Orgánica de Protección de Datos Personales (LOPDP) has a direct and significant operational impact on how such systems must be designed, deployed, and governed.

1.3.1 Limitación a la toma de decisiones totalmente automatizadas

El Artículo 20 reconoce el derecho **a no ser objeto de una decisión basada única o parcialmente en tratamientos automatizados**, incluida la creación de perfiles, cuando estas decisiones afecten de manera significativa sus derechos y libertades fundamentales; esta disposición prohíbe el despliegue de *flujos de decisión completamente autónomos* en contextos de alto impacto, tales como:

- Rechazo automatizado de postulantes a un empleo.
- Denegación automatizada de créditos o préstamos.
- Sistemas de puntuación automatizada que incidan directamente en oportunidades contractuales o económicas.

Entonces, el responsable del tratamiento no puede basarse exclusivamente en los resultados creados por un algoritmo para adoptar decisiones vinculantes, a no ser que se establezca una configuración alguna de las excepciones del Artículo 20.

1.3.2 Intervención humana y supervisión obligatoria

Desde un punto de vista más operativo, el Artículo 20 obliga a los responsables a incorporar una **intervención humana** dentro del flujo de toma de decisiones.

Esta exigencia deriva de los derechos que se otorgan al titular de los datos:

1. Solicitar una **explicación motivada** de la decisión adoptada;
2. Presentar **observaciones** respecto de la decisión automatizada;

3. Obtener información sobre los **criterios de valoración** utilizados por el sistema automatizado;
4. Impugnar la decisión ante el responsable o encargado del tratamiento.

Para garantizar estos derechos, la organización se debe asegurar que un decisor humano calificado:

- Revise la recomendación generada por el sistema automatizado,
- Tenga la facultad real de modificar o revocar el resultado algorítmico,
- Pueda proporcionar al titular una justificación razonada y comprensible de la decisión final.

Una intervención humana meramente formal, o simbólica, no cumple con las exigencias de la LOPDP, especialmente a la luz de los principios de **transparencia**, **proporcionalidad** y **aplicación favorable al titular** establecidos en el Artículo 10.

1.3.3 Impacto en la arquitectura y gobernanza del sistema

Desde una perspectiva técnica, se puede decir que este derecho obliga a rediseñar los sistemas de inteligencia artificial para incorporar:

- Arquitecturas de tipo *human-in-the-loop* o *human-on-the-loop*,
- Registros de auditoría y mecanismos de trazabilidad de las decisiones automatizadas.
- Mecanismos de explicación que permitan comprender la lógica general y las fuentes de datos utilizadas por el modelo.
- Procedimientos para atender impugnaciones y recursos dentro de los plazos legales.

El Artículo 20 de la LOPDP transforma sistemas de toma de decisiones automatizadas de herramientas puramente técnicas en **sistemas sociotécnicos**, en los cuales: el juicio humano, la rendición de cuentas y la supervisión efectiva son requisitos legales obligatorios; esto incrementa la complejidad operativa y los costos de cumplimiento para organizaciones que implementan IA en contextos con un alto riesgo.

1.4 Under what conditions is the international transfer of personal data restricted by the LOPDP?

La LOPDP no prohíbe de forma absoluta la transferencia internacional de datos personales, sin embargo, establece un conjunto de condiciones estrictas que, en la práctica, **restringen y condicionan** este tipo de operaciones.

1.4.1 Aplicación extraterritorial y sujeción a la LOPDP

Según el Artículo 3, la ley se aplica incluso cuando el encargado del tratamiento se encuentre fuera del Ecuador, siempre que:

- Se traten datos personales de titulares que residan en el Ecuador.
- El tratamiento esté relacionado con la oferta de bienes o servicios a dichos titulares.

Cualquier transferencia de carácter internacional de datos personales que involucre titulares ecuatorianos queda sujeta a las obligaciones, principios y derechos de la LOPDP, independientemente de la ubicación geográfica.

1.4.2 Requisitos de licitud y consentimiento informado

De acuerdo con los Artículos: 7, 8 y 33:

- No existe una **base de legitimidad** válida para el tratamiento (consentimiento, obligación legal, contrato, interés público o interés legítimo debidamente justificado);
- No se cuenta con el **consentimiento libre, específico, informado e inequívoco** del titular, cuando este sea requerido;
- La finalidad de la transferencia no ha sido informada previamente al titular o no es compatible con la finalidad original del tratamiento.

El consentimiento se considera informado únicamente si el titular conoce expresamente que sus datos serán transferidos a un tercero ubicado en el extranjero, la finalidad de dicha transferencia y el tipo de actividad que realiza el destinatario.

1.4.3 Transferencias a terceros y encargados fuera del país

Según los Artículos 33 a 36, la transferencia internacional de datos personales está restringida cuando:

- El acceso del tercero no se encuentra debidamente regulado mediante un contrato que limite el tratamiento a las instrucciones del responsable;
- El destinatario pretende reutilizar los datos para finalidades propias o secundarias;
- No existen mecanismos para asegurar la eliminación o devolución de los datos una vez cumplida la finalidad del servicio.

En estos casos, aun cuando el destinatario se encuentre en el extranjero, la LOPDP es obligatoria para él por el solo hecho de recibir los datos personales, salvo que estos hayan sido debidamente anonimizados.

1.4.4 Datos sensibles y categorías especiales

La transferencia internacional de datos sensibles, datos de salud o datos de niñas, niños y adolescentes se encuentra **especialmente restringida** (Arts. 25 y 26). Este tipo de transferencia solo es lícita cuando:

- Existe consentimiento explícito del titular o de su representante legal;
- Se justifica por razones de interés público esencial;
- Se adoptan salvaguardas reforzadas, como anonimización o seudonimización.

1.5 Explain the role of the Data Protection Authority (DPA) regarding international data transfers. How does this requirement create operational friction or regulatory compliance barriers for a multinational AI company that typically relies on centralized cloud infrastructure outside of Ecuador?

La LOPDP le atribuye a la DPA un rol central en la supervisión de las transferencias internacionales de datos personales, para garantizar el respeto de los principios del tratamiento de los derechos de los titulares, incluso cuando el tratamiento se realiza fuera del territorio ecuatoriano.

En ejercicio del principio de *responsabilidad proactiva*, la DPA puede exigir al responsable del tratamiento que acredite que existe una base jurídica válida, la conservación de la finalidad original del tratamiento y la adopción de garantías adecuadas por parte del destinatario extranjero.

Para una empresa multinacional de inteligencia artificial que opera con infraestructuras cloud fuera del Ecuador, estas exigencias generan fricciones operativas de cumplimiento relevantes, limitando el uso de esquemas de entrenamiento de modelos, obligan a implementar segmentación geográfica y trazabilidad de los datos de titulares ecuatorianos.

La intervención de la DPA condiciona el diseño de sistemas de inteligencia artificial, restringiendo la libre circulación de datos personales hacia infraestructuras extranjeras y reforzando la soberanía de los datos.

2 Corporate Policy Scrutiny: The Data Repurposing Conflict

2.1 Select two major generative AI providers (e.g., OpenAI, Meta, or Anthropic). Briefly summarize how each company differentiates the data usage practices between their Enterprise/API Services (for paying business clients) and their Consumer/Chatbot Services (for free public users) regarding model training.

Para analizar este conflictos de datos y las de limitación de finalidad y consentimiento explícito, se seleccionaron dos servicios que han incurcionado inteligencia artificial generativa: **OpenAI** y **Meta**. Ambos adoptan modelos de negocio diferentes respecto al uso de datos personales para el entrenamiento de modelos, lo que permitirá contrastar sus enfoques frente a la LOPDP.

2.1.1 OpenAI: diferenciación explícita entre servicios empresariales y de consumo

OpenAI establece una separación entre sus servicios empresariales y su servicio de consumo.

En el caso de **ChatGPT y los servicios API**, la política corporativa nos indica que los datos proporcionados por clientes de pago **no se utilizan para entrenar modelos** por defecto, dichos datos permanecen bajo control del cliente, con garantías contractuales de confidencialidad y limitación de finalidad.

En contraste, el servicio de (**ChatGPT gratuito**), puede utilizar el contenido de las conversaciones, junto con información de cuenta y datos técnicos, para mejorar y entrenar sus modelos, salvo que el usuario ejerza un mecanismo de exclusión voluntaria (*opt-out*), reflejando un modelo en el que la protección de datos depende del tipo de usuario.

2.1.2 Meta: integración de IA generativa en servicios de consumo

Meta no ofrece una separación clara entre servicios de inteligencia artificial empresariales y servicios de consumo, ya que sus capacidades de IA generativa están integradas en Facebook, Instagram, Messenger y WhatsApp, nutriéndose principalmente del contenido generado por usuarios.

Las políticas indican que la información compartida por los usuarios, como texto, imágenes, audio, video y metadatos, puede ser utilizada para desarrollar, mejorar y entrenar sistemas de inteligencia artificial y aprendizaje automático. Esta práctica se enmarca en finalidades amplias de investigación, mejora de productos y desarrollo de nuevas funcionalidades, sin una distinción explícita entre datos para la prestación del servicio y datos reutilizados para entrenamiento de modelos.

2.1.3 Comparación y relevancia jurídica

OpenAI adopta un modelo de **segmentación**, donde el uso de datos para entrenamiento depende del tipo de servicio contratado, mientras que Meta sigue un modelo de **integración total**, en el cual los datos de usuarios de servicios gratuitos alimentan de forma generalizada el desarrollo de sistemas de IA.

Desde la perspectiva de la LOPDP, ambos modelos presentan riesgos, pero el enfoque de Meta plantea un conflicto estructural más profundo con los principios de finalidad y consentimiento explícito, al basar el entrenamiento de IA en datos recolectados originalmente para fines sociales.

Criterio	**OpenAI**	**Meta**
Tipo de servicios	Servicios diferenciados (Enterprise/API vs. Consumer)	Ecosistema integrado (redes sociales + Meta AI)
Usuarios principales	Empresas (servicios de pago) y público general (servicio gratuito)	Principalmente usuarios gratuitos
Uso de datos para entrenamiento	Enterprise/API: no se utilizan por defecto Consumer: sí, salvo mecanismo de *opt-out*	Uso amplio de contenido generado por usuarios
Separación entre consumo y entrenamiento	Clara y explícita	Débil o inexistente
Modelo de consentimiento	Exclusión voluntaria posterior (*opt-out*) en servicios de consumo	Configuración posterior y control fragmentado
Riesgo frente a la LOPDP	Alto en servicios de consumo	Alto y estructural

Table 1: Comparación entre OpenAI y Meta respecto al uso de datos para entrenamiento de modelos de IA

2.2 Analyze the public-facing policy for the consumer chat version of one of your selected companies. Identify the type of user input data (e.g., chat content, account info, technical data) that may be used for model training.

Para este análisis, se examinó la política de privacidad del servicio de chat de consumo de **OpenAI**, en tanto se trata de un servicio gratuito orientado al público general y representa un caso casi paradigmático de reutilización de datos personales para el entrenamiento.

De acuerdo con la política de OpenAI, el servicio de consumo recopila y puede utilizar diversas categorías de datos personales proporcionados directa o indirectamente por los usuarios:

- **Contenido del usuario**: comprende mensajes enviados en las conversaciones, así como archivos, imágenes, audio y otros contenidos cargados.
- **Información de la cuenta**: incluye datos identificativos y administrativos como: nombre, información de contacto, credenciales de acceso, fecha de nacimiento, información de pago e historial de transacciones, cuando el usuario crea una cuenta.
- **Información de comunicación**: corresponde a los datos del usuario cuando se comunica con OpenAI por correo, redes sociales u otros canales de soporte.
- **Información técnica**: abarca datos tales como dirección IP, tipo y configuración del navegador, fechas y horas de acceso, zona horaria, país, tipo de dispositivo, sistema operativo, identificadores del dispositivo, datos de interacción con el servicio y cookies.
- **Información de ubicación**: se refiere a la ubicación aproximada inferida a partir de la dirección IP, así como información de ubicación más precisa cuando el usuario decide proporcionarla voluntariamente.

La política establece que OpenAI puede usar el **contenido proporcionado por los usuarios del servicio de consumo** para *mejorar y desarrollar sus servicios*, lo que incluye el **entrenamiento de los modelos que impulsan ChatGPT**. Este uso se realiza como regla general, a no ser que el usuario ejerza un mecanismo de exclusión voluntaria.

En contraste, la política aclara que los contenidos procesados en nombre de clientes de servicios **Business o API** no se tienen relación con esta política y no se utilizan para entrenamiento.

2.3 Describe the practical process a user must follow to opt out of having their data used for training (e.g., submission of a form, navigation of settings, or use of a specific toggle).

Los mecanismos para excluir el uso de datos personales en el entrenamiento de modelos de IA tienen diferencias relevantes entre OpenAI y Meta, tanto en su claridad como en su accesibilidad para el usuario.

2.3.1 OpenAI (ChatGPT)

La política de privacidad de OpenAI establece que el contenido generado por los usuarios del servicio de consumo de ChatGPT puede ser utilizado para mejorar y entrenar sus modelos. No obstante, el usuario puede ejercer un *opt-out* mediante una acción posterior.

En la práctica, el usuario debe acceder a la configuración de su cuenta o presentar una solicitud expresa a través del portal de privacidad de OpenAI o por correo electrónico, solicitando que su contenido no sea utilizado con fines de entrenamiento. El uso de los datos para entrenamiento opera por defecto, salvo oposición expresa del titular.

2.3.2 Meta

En el ecosistema de Meta, no existe un mecanismo específico y unificado para excluir el uso de datos personales en el entrenamiento de sistemas de inteligencia artificial. Las políticas indican que el contenido generado por los usuarios puede ser utilizado para desarrollar y mejorar productos, incluyendo sistemas de IA.

El control del usuario se limita a herramientas generales de privacidad, como la gestión de contenido o el ejercicio de derechos de acceso y eliminación, sin un *opt-out* claro, directo y específico respecto al entrenamiento de modelos.

2.4 Critically evaluate: How does this opt-out mechanism conflict with the LOPDP's mandate for prior, informed, and explicit consent for data processing?

Los mecanismos de *opt-out* utilizados en OpenAI y Meta entran en conflicto con el estándar de consentimiento establecido en la LOPDP, exigiendo que el tratamiento de datos personales se base en un consentimiento **previo, informado, y específico**.

Para empezar, el uso de datos para el entrenamiento de modelos de inteligencia artificial se activa *por defecto*, trasladando al titular la carga de oponerse posteriormente al tratamiento. Esto resulta incompatible con el carácter *previo* del consentimiento exigido por la LOPDP, pues el tratamiento comienza antes de que el titular manifieste una voluntad afirmativa.

En segundo lugar, el consentimiento no puede considerarse *específico* cuando la exclusión requiere acciones adicionales, como la navegación por configuraciones complejas o la presentación de solicitudes formales y la LOPDP exige una manifestación clara e inequívoca de voluntad.

Asimismo, el carácter *informado* del consentimiento se ve debilitado por la formulación amplia y técnica de las políticas de privacidad, que no distinguen de manera suficientemente clara entre el uso de los datos para la prestación del servicio y su reutilización para entrenamiento de modelos.

Desde el principio de **limitación de finalidad**, el entrenamiento de modelos constituye una finalidad secundaria distinta de la interacción directa con el servicio. La LOPDP no permite que dicha reutilización se fundamente en mecanismos de oposición posterior.

Los modelos de *opt-out* analizados priorizan la eficiencia operativa y el escalamiento de sistemas de IA sobre las garantías sustantivas de protección de datos, generando un riesgo elevado de incumplimiento de la LOPDP en servicios de consumo masivo.

2.5 Legal Risk Scenarios: Research a recent legal challenge or public controversy where an AI company (e.g., Meta, LinkedIn, or Amazon) was accused of using previously collected user-generated content or biometric data for a new, secondary AI training purpose without proper consent. Briefly summarize the nature of the alleged violation (e.g., biometric privacy, repurposing of communication data).

Para comenzar, puede destacarse un caso relevante y debidamente documentado que involucra a **Meta Platforms, Inc.** y la recolección, almacenamiento y uso no autorizado de **datos biométricos** de los usuarios de sus plataformas, particularmente en el contexto de tecnologías de reconocimiento facial.

En febrero de 2022, el Fiscal General del estado de Texas inició una acción legal contra Meta por la captura y utilización de datos biométricos personales —incluidos identificadores de geometría facial extraídos de fotografías— pertenecientes a millones de residentes, sin haber obtenido el **consentimiento previo, informado y expreso** exigido por la legislación estatal aplicable [4].

El problema principal fue que las fotos se compartieron originalmente para un fin simple, como publicar contenido o etiquetar amigos, pero luego se usaron para un propósito distinto: entrenar sistemas de inteligencia artificial. Los usuarios no fueron informados claramente de este nuevo uso ni se les pidió autorización expresa, lo que generó una fuerte controversia legal.

Este caso muestra cómo reutilizar información personal para entrenar inteligencia artificial, sin avisar ni pedir permiso adecuado, puede causar graves problemas legales para las empresas tecnológicas.

3 Technical Risk Assessment and Mitigation

Los sistemas de AI que procesan datos presentan riesgos técnicos que pueden desencadenar daños graves a los derechos de los titulares. En esta sección se analizan escenarios concretos de riesgo asociados a sistemas de alto impacto, vinculándolos con los principios y derechos establecidos en la LOPDP.

3.1 High-Risk Application Scenario: Predictive Policing Systems

Un ejemplo de aplicación de riesgo podría ser la implementación de un sistema de **policía predictiva** basado en inteligencia artificial. Este tipo de sistema utilizaría datos históricos de reportes policiales para predecir zonas, horarios o personas con mayor probabilidad de cometer delitos.

El principal riesgo surge entonces cuando los datos de entrenamiento reflejan prácticas policiales históricamente sesgadas, como por ejemplo, una mayor presencia y control en barrios empobrecidos. Al aprender de estos datos, el sistema tiende a reforzar dichos patrones, generando una vigilancia desproporcionada sobre los mismos grupos sociales.

Este funcionamiento puede producir **efectos discriminatorios**, como mayor probabilidad de controles, detenciones o estigmatización, basados solo en decisiones automatizadas. Desde la perspectiva de la LOPDP, esta situación vulnera el **principio de proporcionalidad y necesidad**, al utilizar datos excesivos y no pertinentes, así como el derecho reconocido en el **Artículo 20**, que garantiza a las personas no ser objeto de decisiones basadas únicamente en valoraciones automatizadas con efectos jurídicos relevantes.

3.2 Technical Security Risk: Model Memorization and Data Leakage

Otro riesgo técnico relevante sería el fenómeno conocido como **model memorization** o **data leakage**, esto ocurre cuando un modelo de IA aprende y conserva información personal específica contenida en los datos utilizados durante su entrenamiento, y posteriormente la reproduce de forma no autorizada.

Supongamos un chatbot utilizado internamente en un hospital, entrenado con ejemplos reales que incluyen información médica de pacientes. Si el sistema memoriza estos datos y, ante una consulta posterior, revela información de salud identificable de un paciente distinto, se produce una divulgación no autorizada de datos sensibles.

Este escenario constituye una vulneración directa del **derecho a la confidencialidad y seguridad de los datos personales**, así como de la protección reforzada aplicable a los **datos de salud**, considerados datos sensibles por la LOPDP.

3.3 Relevancia para la gobernanza y mitigación de riesgos

Estos escenarios demuestran que los riesgos de la IA no son únicamente teóricos, ya que pueden materializarse a partir de decisiones técnicas como la selección de datos de entrenamiento, la ausencia de supervisión humana o la falta de controles de seguridad.

Desde la perspectiva de la LOPDP, estos riesgos obligan a las organizaciones a incorporar medidas de mitigación desde el diseño de los sistemas, tales como: evaluación de sesgos en los datos, supervisión humana efectiva, minimización de datos y controles de acceso estrictos.

4 Bibliografía

References

[1] Consejo de Regulación y Desarrollo de la Información y Comunicación (CORDICOM), *Ley Orgánica de Protección de Datos Personales (LOPDP)*, 2021, Disponible en: https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

[2] OpenAI OpCo, LLC, *Política de Privacidad — OpenAI (ChatGPT)*, Disponible en: https://openai.com/es-419/policies/row-privacy-policy/

[3] Meta Platforms, Inc., *Política de Privacidad — Meta*, Disponible en: https://www.facebook.com/privacy/policy/

[4] Office of the Attorney General of Texas, *Attorney General Ken Paxton Secures $1.4 Billion Settlement from Meta Over Its Unauthorized Capture of Personal Biometric Data*, 2024, Disponible en: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture