Módulo 4. Gestión de datos y privacidad en entornos mobile

Gestión de datos y privacidad en entornos mobile

En los entornos digitales actuales, las aplicaciones móviles se configuran como espacios donde la interacción cotidiana de las personas genera flujos constantes de información. Cada acción —desde abrir una aplicación hasta realizar una compra o compartir contenido— implica la producción y circulación de datos que deben ser gestionados de manera adecuada. En este contexto, la **gestión de datos** y la **privacidad** adquieren una dimensión operativa dentro del desarrollo de productos digitales, ya que influyen directamente en la forma en que se diseñan experiencias, se configuran funcionalidades y se establecen relaciones con las personas usuarias.

A medida que los modelos de negocio digitales incorporan estrategias basadas en datos, se vuelve necesario comprender cómo se recolecta, procesa y utiliza esa información dentro de las aplicaciones. La implementación de mecanismos como el *consent management* o el uso estratégico de *first-party data* plantea desafíos concretos en el diseño de interfaces y en la toma de

decisiones. En ese marco, surge una pregunta relevante: ¿de qué manera se pueden integrar prácticas de recolección de datos que resulten funcionales para el negocio y, al mismo tiempo, respeten las condiciones de uso aceptadas por las personas usuarias?

Desde una perspectiva profesional, estas decisiones no se limitan a aspectos técnicos, sino que involucran criterios vinculados a la **transparencia**, la claridad en la comunicación y la coherencia entre lo que la aplicación solicita y lo que efectivamente realiza con la información. La configuración de permisos, los avisos de uso de datos y las instancias de aceptación forman parte de la experiencia de uso, y su diseño impacta tanto en la comprensión como en la disposición de las personas a interactuar con la aplicación. De este modo, la privacidad se integra como un componente del diseño de producto, y no como una instancia separada o posterior.

En este bloque abordaremos los principios y prácticas vinculadas a la **gestión del consentimiento** y al uso de datos propios como recurso estratégico. A través del análisis de estos componentes, se busca comprender cómo se articulan las decisiones de diseño, las necesidades del producto y las expectativas de las personas usuarias en entornos donde la información constituye un recurso central. Este enfoque permite situar la privacidad como parte del proceso de desarrollo, integrando criterios técnicos y operativos en la construcción de experiencias digitales sostenibles.

CONSENT MANAGEMENT EN APLICACIONES MOBILE

La **gestión de consentimiento** o *consent management* refiere al conjunto de prácticas, herramientas y decisiones que permiten solicitar, registrar y administrar las preferencias de las personas usuarias respecto al uso de sus datos dentro de una aplicación. En entornos ***mobile***, esta gestión se integra directamente en la experiencia de uso, ya que cada interacción puede implicar la recolección de información personal. Según lo expuesto por Adjust, las organizaciones que trabajan con datos deben presentar opciones claras de privacidad y obtener el consentimiento correspondiente para su tratamiento, lo que posiciona a este proceso como parte del diseño operativo del producto digital.

Desde una perspectiva técnica, las *consent management platforms* (**CMP**) permiten externalizar esta gestión, centralizando la recopilación y administración del consentimiento. Estas plataformas ofrecen configuraciones prediseñadas que facilitan la implementación de mensajes de privacidad y aseguran que las preferencias de las personas usuarias se respeten en todos los puntos de contacto. Además, como se observa en el contenido analizado, las CMP actúan como intermediarias entre la aplicación y sus socios —por ejemplo, redes publicitarias—, compartiendo el estado del consentimiento mediante integraciones como *SDK*, lo que habilita decisiones automatizadas sobre el uso de datos en tiempo real (Adjust, 2026).

La gestión del consentimiento se articula con distintos tipos de autorización: el consentimiento **explícito**, cuando la persona usuaria acepta de forma directa; el **implícito**, cuando se infiere a partir del uso de la aplicación; y el **informado**, cuando se brinda información clara sobre el uso de los datos antes de su aceptación. Cada uno de estos tipos implica

diferentes niveles de intervención en el diseño de interfaces y en la comunicación con las personas usuarias, lo que incide en la forma en que se estructuran los flujos de interacción dentro de la aplicación.

A nivel de implementación, el desafío consiste en integrar estos mecanismos sin interrumpir la experiencia de uso. Tal como señala Adjust, los mensajes de privacidad deben formar parte de una experiencia fluida, evitando generar fricción o abandono. Esto implica diseñar elementos como ***banners***, solicitudes de permisos y pantallas de configuración que comuniquen de manera clara y coherente, manteniendo alineados los objetivos del producto con las expectativas de privacidad de las personas usuarias.

Tabla 1. Tipos de consentimiento en aplicaciones *mobile* y sus características

Tipo de consentimiento	**Forma de obtención**	**Nivel de intervención del usuario**	**Aplicación en entornos *mobile***
Explícito	Aceptación directa mediante acción (***clic***, ***check***)	Alto	Permisos de acceso (ubicación, cámara)
Implícito	Derivado del uso o navegación	Medio	Uso continuo de funcionalidades
Informado	Aceptación basada en	Alto	Políticas de privacidad y avisos iniciales

	información previa clara		

Fuente: elaboración propia con base en Adjust (2026)

A partir de esta clasificación, se observa que cada tipo de consentimiento requiere decisiones específicas en el diseño de interfaces. Por ejemplo, el consentimiento explícito suele resolverse mediante acciones claras dentro de la aplicación, mientras que el informado demanda instancias de comunicación que expliquen el uso de los datos antes de su aceptación. Esta diferenciación impacta en la estructura de los flujos de navegación y en la manera en que se presentan los contenidos vinculados a la privacidad.

En el plano operativo, las CMP facilitan la gestión de estas variantes al ofrecer plantillas configurables que se adaptan a distintos marcos regulatorios y contextos de uso. Según Adjust, estas plataformas permiten mantener coherencia en la comunicación de preferencias y evitar la repetición innecesaria de solicitudes, lo que contribuye a reducir la fatiga asociada al consentimiento en múltiples dispositivos. Este aspecto resulta relevante en entornos donde las personas interactúan con una misma marca desde distintos canales.

Por otra parte, la integración técnica mediante ***SDK*** permite que la información sobre el consentimiento se comparta con distintos actores del ecosistema digital. De este modo, cada sistema puede determinar si dispone de autorización para utilizar determinados datos, asegurando que las acciones posteriores —como la personalización de contenidos o la medición de campañas— se alineen con las preferencias registradas. Esta lógica conecta la experiencia de usuario con los procesos internos de gestión de datos.

Finalmente, la implementación efectiva del ***consent management*** implica articular tres dimensiones: la comunicación clara con las personas usuarias, la configuración técnica de los sistemas y la coherencia en el uso de los datos. Esta integración permite que la gestión del consentimiento funcione como un componente estructural del producto digital, alineando la operación técnica con los criterios de privacidad definidos.

Figura 1. Flujo de gestión de consentimiento en aplicaciones *mobile*


Usuario interactúa con la app
Solicitud de consentimiento
Procesamiento en CMP
Registro de preferencias
Compartición con socios vía SDK
Uso de datos según consentimiento

Fuente: elaboración propia con base en Adjust (2026)

Este flujo permite comprender cómo la gestión del consentimiento se integra en la operación diaria de una aplicación, conectando la interacción inicial de la persona usuaria con decisiones automatizadas sobre el uso de datos. Cada etapa del proceso responde a una lógica de validación continua, donde las preferencias registradas condicionan las acciones posteriores dentro del ecosistema digital.

En términos de práctica profesional, esta articulación entre experiencia de usuario y procesamiento técnico habilita el diseño de aplicaciones que operan con criterios claros de **privacidad** y trazabilidad. La capacidad de registrar, actualizar y compartir el estado del consentimiento en tiempo real permite sostener coherencia entre lo que la aplicación comunica y lo que efectivamente ejecuta en relación con los datos.

FIRST-PARTY DATA COMO ACTIVO ESTRATÉGICO

El ***first-party data*** refiere a la información que una organización obtiene directamente a partir de la interacción con sus propias personas usuarias dentro de sus entornos digitales. Este tipo de datos incluye comportamientos de navegación, historial de compras, respuestas a campañas e interacciones con contenidos, lo que permite construir un conocimiento situado sobre las dinámicas reales de uso. A diferencia de modelos anteriores basados en datos externos, el enfoque actual sitúa a los datos propios como base de las decisiones estratégicas en contextos ***mobile***, donde cada interacción se convierte en una fuente directa de información relevante.

El desplazamiento hacia el uso de **datos propios** responde a transformaciones en el ecosistema digital, vinculadas a cambios regulatorios y a la creciente centralidad de la privacidad. Según el material analizado, la eliminación progresiva de mecanismos como las cookies de terceros redefine las estrategias de recolección y obliga a las organizaciones a construir sus propios sistemas de datos. En este escenario, el crecimiento sostenido se apoya en la capacidad de gestionar información directa de manera estructurada, integrando fuentes y garantizando coherencia en su uso (HOOD INT, 2026).

En términos operativos, el valor del ***first-party data*** se expresa cuando la información recolectada se activa dentro de los procesos de negocio. Esto implica integrar datos entre plataformas, utilizarlos en campañas y traducirlos en acciones concretas dentro de la experiencia de usuario. La acumulación de datos sin aplicación directa limita su impacto, mientras que su uso estratégico permite mejorar indicadores como la conversión, la fidelización y la eficiencia en la adquisición de usuarios.

Desde una perspectiva de producto, el uso de datos propios se vincula con la construcción de relaciones sostenidas con las personas usuarias. La

posibilidad de personalizar experiencias, anticipar comportamientos y ajustar propuestas de valor se apoya en la calidad y consistencia de la información disponible. En este sentido, el ***first-party data*** se articula con dimensiones como la **confianza**, la **transparencia** y la **personalización**, que configuran el vínculo entre la aplicación y sus usuarios en el largo plazo.

Tabla 2. Tipos de datos en entornos digitales y sus características

Tipo de dato	Origen	Nivel de control	Aplicación estratégica
First-party data	Interacción directa con usuarios	Alto	Personalización, fidelización
Second-party data	Datos compartidos entre socios	Medio	Alianzas estratégicas
Third-party data	Proveedores externos	Bajo	Segmentación masiva

Fuente: elaboración propia con base en HOOD INT (2026)

A partir de esta clasificación, se observa que el ***first-party data*** presenta un mayor nivel de control y trazabilidad en comparación con otras fuentes. Esto permite a las organizaciones definir con mayor precisión cómo se recolecta, almacena y utiliza la información, alineando estos procesos con sus objetivos de negocio y con las expectativas de privacidad de las personas usuarias.

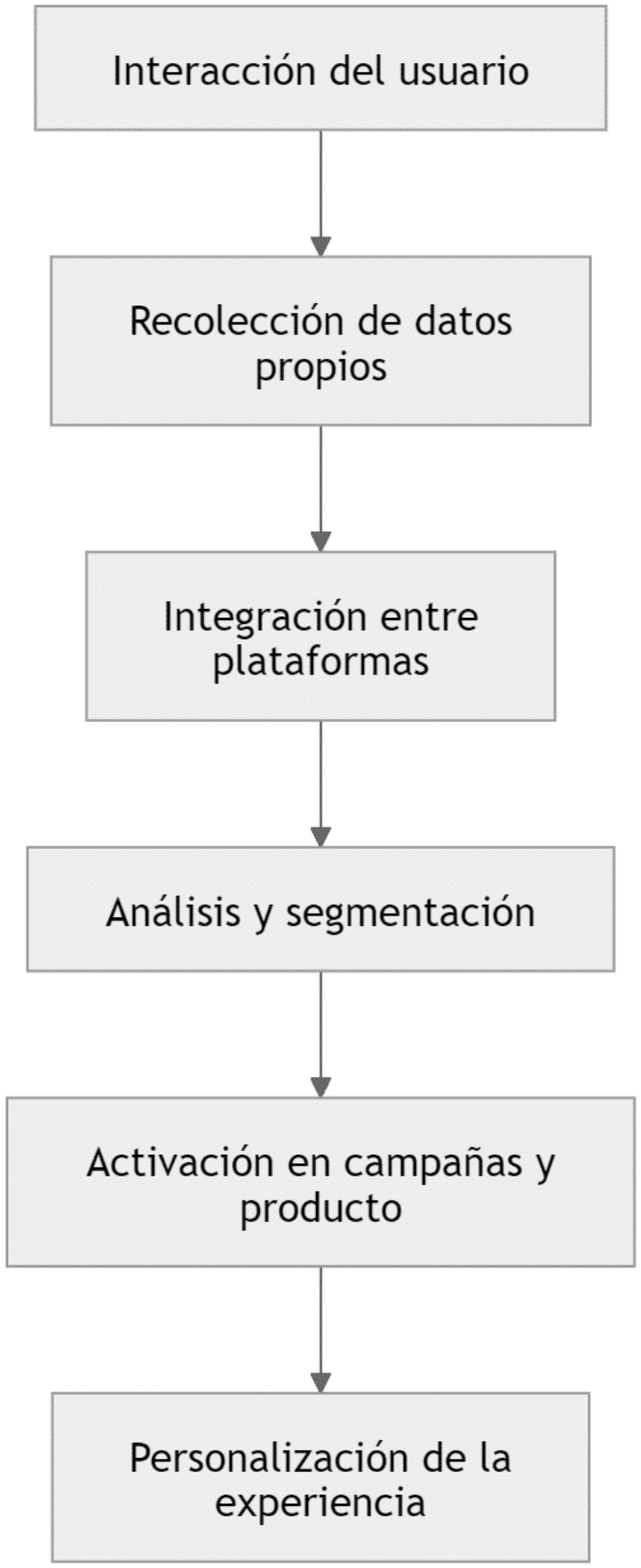
En el plano operativo, la gestión de datos propios requiere la integración de múltiples puntos de contacto dentro del ecosistema digital. Cada interacción —desde el uso de una funcionalidad hasta la respuesta a una campaña— aporta información que debe ser organizada de manera

coherente para facilitar su activación posterior. Esta integración permite construir una visión unificada del usuario, condición necesaria para diseñar experiencias consistentes.

Por otra parte, el uso estratégico del ***first-party data*** impacta directamente en la eficiencia de las acciones de marketing. Tal como se señala en el material, cuando estos datos se utilizan de forma integrada, se mejora la conversión, se reduce el costo de adquisición y se fortalecen los vínculos con las personas usuarias. Este enfoque desplaza el foco desde la captación masiva hacia la gestión relacional basada en información contextual.

Finalmente, la dimensión ética adquiere relevancia en la gestión de datos propios. La comunicación sobre el uso de la información, la claridad en las condiciones de recolección y el valor ofrecido a cambio de los datos inciden en la percepción de las personas usuarias. La **confianza del usuario** se configura como un activo que sostiene el crecimiento a largo plazo, articulando prácticas de datos con criterios de responsabilidad en el diseño de productos digitales.

Figura 2. Flujo de activación del *first-party data* en entornos *mobile*


Interacción del usuario
Recolección de datos propios
Integración entre plataformas
Análisis y segmentación
Activación en campañas y producto
Personalización de la experiencia

Fuente: elaboración propia con base en HOOD INT (2026)

Este flujo permite comprender cómo los datos propios se transforman en insumos para la toma de decisiones dentro del producto digital. Cada etapa del proceso articula la captura de información con su uso operativo, generando una continuidad entre la interacción del usuario y la personalización de la experiencia.

En términos de práctica profesional, la gestión del *first-party data* implica diseñar sistemas que aseguren la calidad, disponibilidad y coherencia de la información. Esta capacidad permite sostener estrategias basadas en conocimiento directo del usuario, reduciendo la dependencia de fuentes externas y fortaleciendo la autonomía en la toma de decisiones.

Construir una estrategia basada en *first-party data* implica organizar, integrar y activar la información obtenida directamente de las personas usuarias a lo largo de sus interacciones con un producto digital. Este enfoque requiere definir puntos de recolección claros, establecer criterios de almacenamiento y diseñar mecanismos que permitan transformar esos datos en acciones concretas. Según el material analizado, el valor de los datos propios se expresa cuando se integran entre plataformas, se utilizan en campañas y permiten personalizar experiencias, lo que desplaza la lógica de acumulación hacia una lógica de **activación de datos**.

En términos operativos, esta estrategia implica construir una infraestructura donde el dato fluye de manera continua entre distintos sistemas. Esto supone articular herramientas de analítica, plataformas de automatización y sistemas de gestión de usuarios, de modo que cada interacción aporte información que pueda ser utilizada en tiempo real o en procesos posteriores. La integración permite consolidar una visión unificada del usuario, condición necesaria para desarrollar acciones coherentes en diferentes canales y momentos del recorrido.

A su vez, el enfoque basado en datos propios redefine la relación entre producto y marketing. En lugar de depender de fuentes externas para segmentar audiencias, las organizaciones desarrollan conocimiento directo sobre el comportamiento de sus usuarios. Este cambio permite diseñar estrategias más ajustadas al contexto de uso, donde la **personalización** se construye a partir de información contextual y no de inferencias generales. De este modo, el marketing se vincula de manera más estrecha con el diseño del producto y con la experiencia de usuario.

En este escenario, el crecimiento deja de centrarse exclusivamente en la captación y se orienta hacia la construcción de relaciones sostenidas. Tal como se señala en el material, el uso adecuado del *first-party data* permite mejorar la conversión, reducir costos de adquisición y fortalecer la fidelización. Esto implica que las decisiones de marketing se apoyan en el conocimiento acumulado sobre los usuarios, generando estrategias más eficientes y alineadas con sus necesidades reales.

Tabla 3. Componentes de una estrategia basada en *first-party data*

Componente	Descripción	Aplicación en marketing *mobile*
Recolección	Captura de datos desde interacciones directas	Formularios, uso de la app
Integración	Unificación de datos entre sistemas	CRM, analítica, automatización
Activación	Uso de datos en acciones concretas	Campañas personalizadas
Evaluación	Medición de resultados	Optimización de conversiones

Fuente: elaboración propia con base en HOOD INT (2026)

A partir de estos componentes, se observa que la estrategia basada en datos propios requiere una coordinación constante entre áreas técnicas y de negocio. La calidad de la información recolectada incide directamente en la efectividad de las acciones de marketing, lo que refuerza la necesidad de procesos integrados y consistentes.

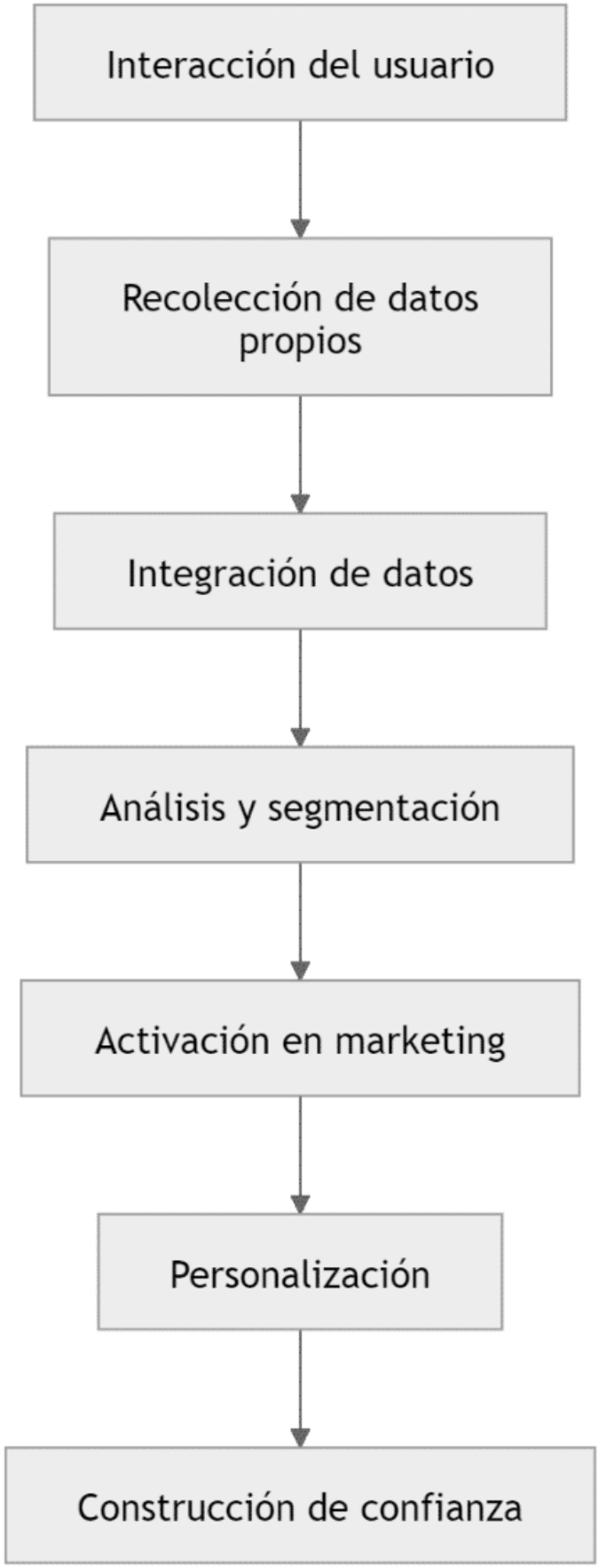
En el contexto actual, caracterizado por mayores restricciones de privacidad, el rol del ***marketing*** experimenta una transformación significativa. La reducción del acceso a datos de terceros y el fortalecimiento de regulaciones obligan a desarrollar estrategias centradas en la **transparencia** y el consentimiento. En este marco, el ***marketing*** se orienta a construir vínculos basados en la confianza, donde la obtención de datos se vincula con la propuesta de valor ofrecida a las personas usuarias.

Este cambio implica que las acciones de ***marketing*** deben justificarse en términos de utilidad para el usuario. La comunicación sobre el uso de los datos, la claridad en las condiciones de acceso y la coherencia en la experiencia influyen en la disposición de las personas a compartir

información. Tal como se plantea en el material, la confianza se convierte en un activo que sostiene el crecimiento, integrando prácticas de datos con decisiones estratégicas.

Finalmente, el ***marketing*** en entornos con restricciones de privacidad se configura como una práctica orientada al conocimiento profundo del usuario. La combinación entre datos propios, análisis contextual y diseño de experiencias permite construir estrategias más sostenibles, donde el crecimiento se apoya en relaciones de largo plazo y en el uso responsable de la información.

Figura 3. Estrategia de marketing basada en *first-party data*


Interacción del usuario
Recolección de datos propios
Integración de datos
Análisis y segmentación
Activación en marketing
Personalización
Construcción de confianza

Fuente: elaboración propia con base en HOOD INT (2026)

Este esquema permite visualizar cómo el marketing se articula con la gestión de datos propios en un entorno regulado. Cada etapa del proceso conecta la interacción con el usuario con decisiones estratégicas orientadas a la personalización y la construcción de relaciones sostenidas.

En términos profesionales, este enfoque redefine las competencias necesarias en marketing, integrando capacidades analíticas, comprensión del comportamiento del usuario y criterios de **privacidad**. La estrategia deja de centrarse en el acceso masivo a datos y se orienta a la gestión eficiente de información propia, alineando objetivos comerciales con prácticas responsables de uso de datos.

CONTINUAR

Diseño responsable y marco regulatorio

En el desarrollo de aplicaciones *mobile*, las decisiones de diseño no se limitan a aspectos funcionales o estéticos, sino que intervienen directamente en la forma en que las personas interactúan, comprenden y toman decisiones dentro de un entorno digital. A medida que los productos incorporan mecanismos de recolección y uso de datos, el diseño comienza a operar como un mediador entre los objetivos del negocio y las condiciones de uso aceptadas por las personas usuarias. En este contexto, prácticas como la configuración de interfaces, la organización de opciones y la presentación de información adquieren una dimensión operativa vinculada a la **experiencia del usuario** y a la **privacidad**.

En articulación con los contenidos del bloque anterior, donde se abordó la gestión del consentimiento y el uso de *first-party data*, se amplía el enfoque hacia las implicancias del diseño en estos procesos. Las decisiones sobre cómo se solicita el consentimiento, cómo se presentan las opciones o cómo se configuran los recorridos dentro de la aplicación inciden

directamente en la comprensión y en la acción de las personas usuarias. De este modo, el diseño deja de ser un componente aislado y se integra como parte del sistema que regula el acceso, uso y circulación de los datos.

En este marco, surgen prácticas que influyen en la toma de decisiones de manera indirecta, como los *dark patterns*, que organizan la interfaz de forma tal que orientan el comportamiento hacia determinadas acciones. Estas configuraciones pueden afectar la claridad de la información, la visibilidad de las opciones y la autonomía en la toma de decisiones. Frente a esto, se desarrollan enfoques de **diseño ético**, que buscan estructurar experiencias donde las personas usuarias puedan comprender, elegir y actuar con información suficiente, en condiciones de transparencia.

Por otra parte, el diseño de productos digitales se encuentra condicionado por marcos regulatorios que establecen criterios sobre el tratamiento de datos personales. Normativas como el *General Data Protection Regulation* (*GDPR*) introducen principios vinculados al consentimiento, la minimización de datos y la transparencia, que deben ser considerados en el diseño de interfaces y flujos de interacción. En este bloque abordaremos cómo se articulan estas dimensiones —**diseño responsable**, regulación y experiencia de usuario— en el desarrollo de

aplicaciones *mobile*, analizando sus implicancias prácticas en la construcción de productos digitales.

Dark patterns vs. diseño ético en *mobile*

Los *dark patterns* o patrones oscuros refieren a decisiones de diseño que orientan la interacción de las personas usuarias hacia acciones específicas mediante mecanismos que condicionan su elección. Estas prácticas surgen en contextos donde se busca optimizar métricas como la conversión o la retención, integrando elementos en la interfaz que influyen en la toma de decisiones. Según el material analizado, se trata de interfaces diseñadas para guiar al usuario hacia caminos que no necesariamente reflejan su intención inicial, lo que introduce una tensión entre objetivos de negocio y criterios de **experiencia de usuario**.

En términos de funcionamiento, los *dark patterns* operan a través de la configuración de opciones, el lenguaje utilizado en los mensajes y la disposición visual de los elementos. Estas decisiones afectan la interpretación de la información y la forma en que se perciben las alternativas disponibles. Por ejemplo, el uso de mensajes que generan presión emocional o la incorporación de condiciones poco visibles en procesos de suscripción modifican la experiencia de interacción, orientando el

comportamiento sin una comprensión completa de las implicancias.

El análisis de estos patrones permite identificar distintas formas de intervención en la interfaz. Entre ellas se encuentran las preguntas engañosas, la incorporación de productos sin consentimiento explícito, la dificultad para cancelar servicios o la inclusión de costos en etapas finales del proceso. Tal como se describe en el documento, estas prácticas se estructuran en categorías que facilitan su reconocimiento y análisis dentro del diseño de productos digitales, lo que resulta relevante para su detección en entornos *mobile*.

Desde una perspectiva de producto, la implementación de estos patrones impacta en la relación con las personas usuarias. La priorización de resultados inmediatos puede afectar la

percepción de la marca y generar efectos en la continuidad del uso. En este sentido, el diseño de interfaces se vincula con dimensiones como la **confianza del usuario**, la claridad en la comunicación y la coherencia entre lo que se presenta y lo que efectivamente ocurre durante la interacción.

Tabla 4. Tipos de *dark patterns* y su impacto en la experiencia de usuario

Tipo de patrón	Descripción	Impacto en la experiencia
Confirmshaming	Mensajes que generan culpa al rechazar una opción	Presión emocional en la decisión
Sneak into basket	Productos añadidos automáticamente	Pérdida de control del usuario
Roach motel	Dificultad para cancelar servicios	Fricción en la salida
Costos ocultos	Cargos agregados al final del proceso	Falta de transparencia

Bait and switch	Resultado distinto al esperado	Confusión y desconfianza

Fuente: elaboración propia con base en Practia (2025)

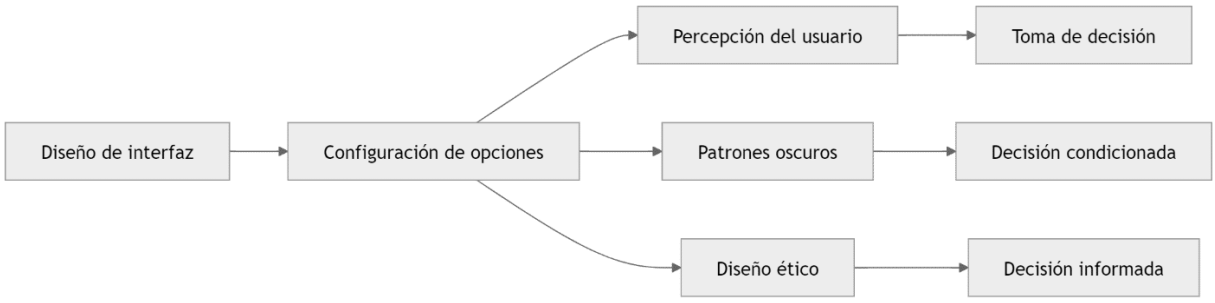
A partir de esta tipificación, se observa que los *dark patterns* comparten una lógica común: intervenir en la toma de decisiones mediante la configuración de la interfaz. Esta intervención se apoya en aspectos visuales, textuales y estructurales que modifican la percepción de las opciones disponibles.

En el plano operativo, estas prácticas pueden integrarse en diferentes momentos del recorrido del usuario: desde el registro inicial hasta los procesos de pago o cancelación. La recurrencia de estos patrones en entornos digitales evidencia la necesidad de desarrollar criterios de análisis que permitan identificarlos y evaluar su impacto en la experiencia.

Por otra parte, el reconocimiento de estos patrones habilita la construcción de enfoques alternativos centrados en el usuario. En lugar de orientar la interacción hacia resultados predeterminados, el diseño puede organizar la información de manera que facilite la comprensión y la toma de decisiones informadas. Esta perspectiva se vincula con el desarrollo de prácticas de **diseño ético**, donde la claridad y la accesibilidad de las opciones adquieren un rol central.

Finalmente, la discusión en torno a los *dark patterns* introduce una dimensión regulatoria y reputacional en el diseño de productos digitales. Tal como se menciona en el material, existen antecedentes de sanciones a organizaciones por el uso de estas prácticas, lo que refuerza la necesidad de considerar criterios éticos en la construcción de interfaces.

Figura 4. Relación entre diseño de interfaz y toma de decisiones del usuario



Fuente: elaboración propia con base en Practia (2025)

Este esquema permite visualizar cómo las decisiones de diseño inciden en la forma en que las personas interpretan y actúan dentro de una aplicación. La estructura de la interfaz condiciona la percepción y, en consecuencia, el tipo de decisión que se produce.

En términos de práctica profesional, la distinción entre *dark patterns* y diseño ético implica evaluar cómo se presentan las opciones y qué grado de control tienen las personas usuarias sobre sus decisiones. Esta evaluación forma parte del proceso de diseño, integrando criterios de **transparencia** y coherencia en la construcción de experiencias digitales.

REGULACIONES DE PRIVACIDAD (GDPR Y CONTEXTO LATAM)

El *General Data Protection Regulation* (*GDPR*) constituye un marco normativo que establece criterios sobre cómo deben recolectarse, procesarse y protegerse los datos personales. Desde su implementación en 2018, este reglamento introdujo un enfoque centrado en los derechos de las personas, incorporando principios como el consentimiento, la **transparencia**, la minimización de datos y la responsabilidad en su tratamiento. Según el material analizado, su alcance extraterritorial implica que no solo regula a organizaciones europeas, sino también a aquellas que procesan datos de personas ubicadas en la Unión Europea, lo que amplía su impacto a nivel global.

En términos operativos, el *GDPR* redefine la forma en que las organizaciones estructuran sus procesos de datos. La necesidad de documentar prácticas, controlar accesos y demostrar cumplimiento introduce una lógica de gestión sistemática de la información. Esto implica responder preguntas concretas sobre qué datos se recolectan, con qué finalidad y bajo qué condiciones se almacenan, lo que transforma la privacidad en un componente integrado a la operación del negocio (Safe-U, 2026).

A partir de estos lineamientos, el *GDPR* se consolida como un modelo de referencia que influye en otras regiones. En América Latina, distintos países han desarrollado o actualizado sus normativas alineándose con estos principios, lo que genera un proceso de convergencia regulatoria. Este fenómeno implica que las organizaciones deben considerar tanto marcos locales como internacionales al diseñar sus estrategias de datos.

Desde una perspectiva de producto digital, estas regulaciones inciden directamente en el diseño de aplicaciones *mobile*. La incorporación de mecanismos de consentimiento, la claridad en las políticas de privacidad y la limitación en la recolección de datos se traducen en decisiones concretas sobre interfaces, flujos y funcionalidades. De este modo, la regulación deja de ser un aspecto externo para integrarse en el proceso de diseño.

Tabla 5. Principios del *GDPR* y su aplicación en entornos *mobile*

Principio	Descripción	Aplicación en apps *mobile*
Consentimiento	Autorización clara del usuario	Permisos explícitos
Transparencia	Información clara sobre el uso de datos	Políticas accesibles
Minimización	Recolección de datos necesarios	Formularios acotados
Seguridad	Protección de la información	Sistemas de resguardo
Responsabilidad	Capacidad de demostrar cumplimiento	Registro de acciones

Fuente: elaboración propia con base en Safe-U (2026)

A partir de estos principios, se observa que el cumplimiento normativo implica integrar la privacidad en cada etapa del ciclo de vida del dato. Esta integración se traduce en decisiones técnicas y de diseño que condicionan la forma en que las aplicaciones gestionan la información de sus usuarios.

En el contexto latinoamericano, la influencia del ***GDPR*** se manifiesta en la creación y actualización de leyes de protección de datos. Países como Brasil, Argentina, Uruguay y Chile han avanzado en marcos regulatorios que incorporan principios similares, promoviendo la alineación con estándares internacionales. Este proceso refleja una tendencia hacia la homogenización de criterios en torno a la privacidad.

Además, organismos regionales como la Red Iberoamericana de Protección de Datos impulsan la adopción de buenas prácticas, facilitando la coordinación entre países. Esta convergencia normativa genera un entorno

donde las organizaciones deben adaptarse a múltiples regulaciones, considerando diferencias locales y similitudes estructurales.

En este escenario, la implementación de regulaciones plantea desafíos vinculados a la gestión operativa de los datos. La necesidad de cumplir con múltiples marcos normativos requiere desarrollar procesos flexibles que permitan adaptarse a distintos contextos regulatorios, manteniendo coherencia en la gestión de la información.

Tabla 6. Regulación de datos: comparación entre GDPR y contexto LATAM

Dimensión	GDPR (Europa)	LATAM
Alcance	Extraterritorial	Principalmente nacional
Enfoque	Derechos del usuario	Alineado con GDPR
Nivel de desarrollo	Consolidado	En evolución
Implementación	Estandarizada	Heterogénea
Coordinación	Alta integración	Coordinación regional en desarrollo

Fuente: elaboración propia con base en Safe-U (2026)

Este panorama evidencia que, si bien existen diferencias en el nivel de madurez normativa, los principios que orientan la protección de datos tienden a converger. Esta convergencia facilita la adopción de estándares comunes en la gestión de la información.

En términos de marketing ***mobile***, estas regulaciones generan un cambio en la forma de diseñar estrategias. La disponibilidad de datos se encuentra condicionada por el consentimiento y por las limitaciones en su uso, lo que requiere desarrollar enfoques basados en datos propios y en relaciones de largo plazo con las personas usuarias.

Finalmente, el impacto del marco regulatorio se expresa en la necesidad de integrar la privacidad como parte del diseño y la operación de productos digitales. La articulación entre regulación, tecnología y experiencia de usuario permite construir entornos donde el uso de datos se realiza de manera coherente con los derechos de las personas y con los objetivos de las organizaciones.

CONTINUAR

Referencias

Adjust. (2026). *Why you need a consent management platform (CMP)*. https://www.adjust.com/blog/consent-management-platforms/

HOOD INT. (2026). *First-party data: la base del growth marketing sostenible en 2026*. https://www.int.com.ar/novedades/marketing-digital/first-party-data-la-base-del-growth-marketing-sostenible-en-2026/

Practia. (2025). *Dark patterns: el oscuro límite entre el resultado y la ética*. https://perspectiva.practia.global/dark-patterns-el-oscuro-limite-entre-el-resultado-y-la-etica/

Safe-U. (2026). *GDPR y Latinoamérica: cómo Europa influyó en las leyes de protección de datos de la región*. https://www.safe-u.com/blog/GDPR-y-latinoamerica-como-europa-influyo-en-las-leyes-de-proteccion-de-datos-de-la-region

CONTINUAR