agencia española protección datos

Autorité de protection des données
Gegevensbeschermingsautoriteit

RECOMENDACIONES Y MEJORES PRÁCTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN VIDEOJUEGOS

Traducción del documento original en inglés "Recommendations and best practices for data protection in video games"

Junio 2026

CONTENIDOS

I. INTRODUCCIÓN

A. ¿QUÉ ES UN VIDEOJUEGO?

Un videojuego es una experiencia digital interactiva en la que uno o varios jugadores interactúan con entornos virtuales mediante un sistema de reglas, objetivos y retroalimentación, generalmente a través de dispositivos electrónicos como ordenadores, consolas, teléfonos inteligentes o plataformas en la nube. Los videojuegos pueden incorporar componentes visuales, auditivos, narrativos y multijugador, lo que permite la competición, la colaboración, la exploración o la creatividad. El concepto de lo que se considera un "videojuego" ha evolucionado más allá de los formatos tradicionales debido a las nuevas tecnologías y experiencias de usuario.

Hoy en día, un videojuego puede incluir los formatos tradicionales que se juegan en consolas, PCs o sistemas portátiles, y que suelen ofrecer gráficos y objetivos complejos y modos multijugador o de campaña. Pero también los juegos móviles, que se juegan en teléfonos inteligentes y tabletas, e incluyen desde juegos casuales "a tu propio ritmo" hasta experiencias multijugador rápidas. También existen los juegos en la nube o por *streaming*, que se distribuyen a través de Internet, para eliminar la dependencia del hardware local para conseguir rendimiento y proporcionar accesibilidad desde distintos dispositivos (teléfonos, televisiones inteligentes, navegadores). También están los juegos en navegador, nativos web (HTML5/JavaScript), que admiten experiencias creadas por los propios jugadores. En un sentido más amplio, existen entornos y plataformas generados por los usuarios, donde los jugadores se convierten en creadores, construyendo y compartiendo sus propios juegos y mundos interactivos. Este modelo es especialmente interesante porque difumina la línea entre jugador y desarrollador.

Además, hay que considerar los juegos de realidad virtual (RV) y realidad aumentada (RA), que se juegan con cascos o dispositivos con capacidad de RA y ofrecen entornos inmersivos o superposiciones sobre el mundo real. Asimismo, los juegos serios y las experiencias altamente gamificadas (simuladores de formación interactivos, aplicaciones de aprendizaje) están diseñados para la educación, el entrenamiento, el aprendizaje, la salud, la terapia o la concienciación, pero siguen clasificándose como videojuegos debido a su estructura interactiva y basada en reglas. Por último, a corto plazo es probable que encontremos en el mercado juegos impulsados por Inteligencia Artificial (IA) y procedimentales, que incluyan personajes autónomos basados en IA, narrativas dinámicas o contenido generativo. Se espera poder crear entornos procedimentales que cambien en cada partida.

En resumen, los elementos clave que definen un videojuego hoy en día son:

1. **Interactividad:** el usuario realiza acciones que generan efectos o respuestas.
2. **Interfaz digital:** se juegan a través de una plataforma digital (a diferencia de los juegos de mesa o físicos puros).
3. **Reglas y objetivos:** están estructurados alrededor de metas con criterios de fracaso/éxito y lógica de juego.
4. **Sistema de retroalimentación:** existe una respuesta en tiempo real basada en elementos visuales, sonidos, puntuaciones, progresión, etc.
5. **Orientación al entretenimiento:** están diseñados principalmente para la diversión, el desafío o la creatividad (incluso si se usan con fines educativos).

B. TAXONOMÍA DE VIDEOJUEGOS

Como ya se ha mencionado, el ecosistema de los videojuegos es increíblemente diverso, desde juegos móviles sencillos hasta títulos complejos, lo que dificulta establecer una única definición y podría beneficiarse de una categorización.

Una taxonomía o clasificación sistemática de los diferentes tipos de videojuegos puede establecerse atendiendo a diferentes dimensiones y características. Estas se corresponden de manera muy natural con las amenazas y riesgos para la protección de datos personales, ya que cada dimensión o característica tiende a modificar qué datos se recogen, por qué se recogen, quién los recibe y lo intrusivo que puede ser su tratamiento. Cuanto más "en línea" sea un juego, por ejemplo, o más basado en arquitecturas en la nube, personalizado o monetizado mediante publicidad y microtransacciones, mayor será el riesgo para la protección de datos personales. Este documento se centra en aquellos videojuegos con el mayor impacto en la protección de datos (ver Tabla 1).

Dimensión	Categoría	Explicación
Orientación	Entretenimiento	Juegos centrados en ofrecer diversión, disfrute y alivio del estrés. Los juegos de entretenimiento buscan cautivar a los jugadores mediante elementos como la narración interactiva, el arte o la música.
	Educación	Juegos diseñados para mejorar habilidades cognitivas, sociales y académicas. Su objetivo es potenciar el aprendizaje mediante la integración de pedagogía y tecnología.
	Juegos serios	Juegos utilizados con fines serios que van más allá del mero entretenimiento, a menudo usados para entrenar a individuos o grupos. Estos juegos suelen modelar actividades físicas del mundo real, entornos o sistemas complejos (herramientas de simulación), permitiendo a los usuarios practicar tareas críticas o rehabilitarse. Esto incluye aplicaciones en ámbitos como los negocios, la atención sanitaria, el transporte (por ejemplo, simuladores de vuelo) o la seguridad.
Conectividad (a menudo relacionada con la dimensión Número de jugadores/Modo de juego)	*Offline* (fuera de línea o desconectado)	Juegos que funcionan independientemente de una conexión continua a Internet, aunque pueden depender de ella en momentos puntuales para actualizaciones, ventas o funcionalidades comunitarias y sociales.
	Online (en línea o conectado)	Juegos que dependen en gran medida de una conexión continua a Internet. Estos juegos aprovechan la conectividad de red para facilitar la competencia, la cooperación y la interacción social entre los jugadores: juegos multijugador y juegos en línea

		masivos (MMO/MMORPG). A menudo requieren servidores centralizados para la persistencia.
Plataforma tecnológica	Dispositivo local	Juegos que se juegan directamente en hardware dedicado propiedad del usuario (consolas, PC, teléfonos móviles, etc.), y suelen basarse en la propiedad física o digital.
	Cloud/streaming	Juegos transmitidos por *streaming* directamente desde servidores remotos a los dispositivos de los usuarios, eliminando la necesidad de hardware local potente o que cumpla con características específicas.
	Realidad virtual y metaverso	Juegos que utilizan hardware altamente especializado (como cascos de realidad virtual) o infraestructuras *online* ubicuas, que crean espacios virtuales compartidos, inmersivos, interactivos y persistentes, yendo más allá de las experiencias de juego tradicionales.
Modelo económico y estrategia de monetización	Pago único	Modelo tradicional basado en la propiedad, que implica un pago único (físico o digital) mediante el cual el consumidor adquiere el juego y lo posee de forma perpetua. Los costes iniciales de estos títulos suelen ser altos, pero otorgan acceso duradero.
	Suscripción	En este modelo los usuarios pagan una cuota recurrente para acceder a un único juego o a un catálogo, a menudo rotatorio, de juegos (o partes de juegos), accesibles desde dispositivos locales (interfaz puramente dentro del juego) o mediante *cloud/streaming* (tiendas oficiales, lanzadores y *storefronts*, etc.).
	Gratis of *Free-to-Play* (F2P)	Este modelo permite a los jugadores acceder al juego de forma gratuita, generando ingresos mediante microtransacciones (pequeñas compras opcionales de bienes y servicios digitales dentro del juego, como monedas virtuales, mejoras o elementos cosméticos), publicidad en el juego (al mostrar mensajes comerciales o anuncios dentro del entorno del juego) u otros métodos de monetización (cajas botín, pase de batalla, etc.). El modelo F2P depende en gran medida de retener a los jugadores para impulsar la monetización a largo plazo.

	Freemium	Este modelo se basa en una combinación de contenido gratuito y *premium*: ofrece acceso gratuito al juego, pero cobra por funcionalidades mejoradas (que pueden incluir pagos únicos o suscripciones).

Tabla 1. Taxonomía de videojuegos

C. CICLO DE VIDA DE UN VIDEOJUEGO Y ACTORES DE LA INDUSTRIA

El ecosistema de los videojuegos consta de roles y actores clave que contribuyen a la creación, distribución, comercialización y consumo de juegos. En general, se pueden encontrar los siguientes actores, resumidos en la Figura 1.

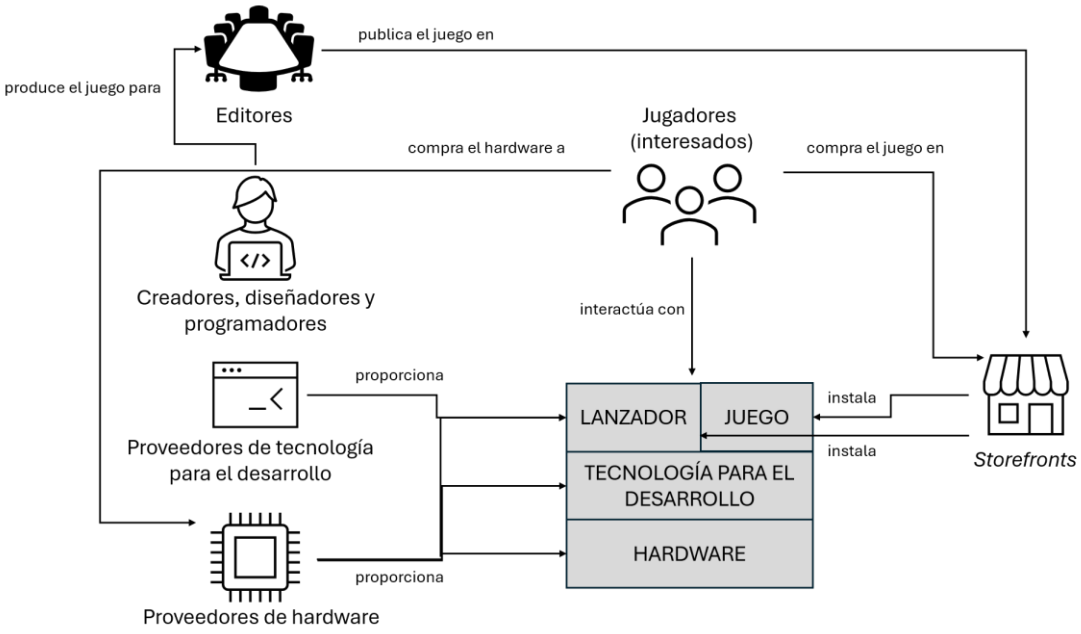

Figura 1. Taxonomía de videojuegos

1. **Proveedores de hardware**: Proporcionan dispositivos físicos que permiten el juego. Esto incluye a fabricantes de consolas, así como a empresas de hardware para PC que producen componentes esenciales, como tarjetas gráficas o periféricos específicos. Estos proveedores crean plataformas y componentes a nivel de sistema (controladores de hardware, pila de red, etc.) en los que se ejecutan los juegos, controlando las licencias, el acceso a la plataforma y, a veces, cobrando derechos de licencia a otros actores por el uso de su hardware.
2. **Creadores, diseñadores y desarrolladores:** Se encargan de la creación y producción real de los videojuegos. Puede que sean individuos o equipos dentro de estudios de desarrollo que diseñan, programan y ensamblan los elementos que componen un juego. Los desarrolladores suelen especializarse en diversos aspectos, como el diseño de juegos (definición de mecánicas de juego, tramas y personajes), la

programación (codificación de la funcionalidad y mecánicas del juego) y la creación artística (elementos visuales, animaciones y recursos).

Se pueden distinguir diferentes tipos de desarrolladores según su relación con los fabricantes de hardware y los editores. Los desarrolladores propios suelen ser equipos internos que trabajan directamente para los fabricantes de consolas, y desarrollan principalmente juegos exclusivos para sus respectivas plataformas. Los desarrolladores de segunda parte son estudios independientes que tienen contratos exclusivos para el desarrollo de juegos para una plataforma específica, pero conservan cierta independencia. Finalmente, los desarrolladores de tercera parte o "terceros" (los únicos que se muestran en la Figura 1 por simplicidad) trabajan para editores externos y pueden desarrollar juegos para múltiples plataformas, generalmente regulados por contratos con hitos estrictos y supervisión del editor.

3. **Proveedores de tecnología para el desarrollo:** Suministran herramientas de software (bibliotecas, *middleware*, kits de desarrollo de software o SDK, interfaces de programación de aplicaciones o API, paquetes de código, motores) que permiten la creación y ejecución de juegos. Sus productos interactúan directamente con los proveedores de hardware para mantener la compatibilidad, mientras que los creadores de juegos dependen de ellos para agilizar el desarrollo. Estas herramientas apoyan a editores y desarrolladores al facilitar la resolución de los retos habituales de producción y ejecución en diferentes equipos y plataformas.
4. **Editores:** Financian, comercializan, distribuyen y, en ocasiones, encargan juegos. Para ello, se coordinan estrechamente con desarrolladores y estudios a fin de gestionar la producción y garantizar que los juegos cumplan los requisitos de plataforma establecidos por los proveedores de hardware. Además, negocian el acceso a *storefronts* para la distribución y supervisan la preparación para el mercado, conectando así los aspectos creativos y comerciales de la industria de los videojuegos.
5. ***Storefronts:*** Son las plataformas de distribución donde los jugadores compran o descargan juegos, actuando como intermediarios entre editores, plataformas de hardware y jugadores como consumidores finales. Estas plataformas trabajan con editores para alojar y promocionar juegos, cumplir con los estándares de los proveedores de hardware y garantizar que los jugadores reciban actualizaciones y soporte, completando así la cadena de distribución. Algunos *storefronts* se centran en el catálogo de un único editor, mientras que otros agrupan juegos de múltiples desarrolladores para una mayor visibilidad y acceso.

   Los lanzadores están estrechamente relacionados con estos *storefronts*. Se trata de aplicaciones dedicadas que funcionan como un concentrador centralizado para comprar, descargar, instalar, actualizar y jugar a los juegos. Estas aplicaciones simplifican el proceso de gestión de archivos de juego de gran tamaño, la aplicación de actualizaciones y el mantenimiento de todos los juegos organizados en un solo lugar, en lugar de obligar a los jugadores a buscar e instalar manualmente parches o gestionar carpetas de instalación separadas para cada juego. Además, muchas de estas aplicaciones ofrecen funcionalidades sociales, como chat, foros, emparejamiento multijugador y logros, lo que ayuda a crear una experiencia de juego enriquecida y a conectar a unos jugadores con otros.

Este ecosistema opera mediante interconexiones constantes entre los distintos actores. Los proveedores de hardware establecen estándares que la tecnología de desarrollo y los desarrolladores deben cumplir. Desarrolladores y editores colaboran para ofrecer productos

atractivos, mientras que los *storefronts* garantizan que los juegos lleguen a los jugadores en diversas plataformas. Estas relaciones superpuestas forman un sistema robusto y dinámico que impulsa la industria global de los videojuegos.

Cabe destacar que las comunidades de jugadores pueden enriquecer los videojuegos mediante la creación de contenido generado por los usuarios (*User Generated Content* o UGC), como *skins*, escenarios, *mods* y mapas, asumiendo así roles de creadores, diseñadores y desarrolladores junto a su función principal como jugadores. Como resultado, los juegos, cade vez más, no son productos fijos de los desarrolladores, sino ecosistemas colaborativos donde los jugadores son coautores de la experiencia. Esta dinámica no es inusual, ya que los actores suelen desempeñar múltiples roles dentro del ecosistema.

Es bastante común que una misma empresa en el ecosistema de los videojuegos desempeñe múltiples roles simultáneamente, especialmente en el caso de grandes empresas o negocios diversificados. Las grandes empresas o editores suelen actuar a la vez como desarrolladores, editores e, incluso, operadores de *storefronts* o proveedores de tecnología para el desarrollo. Los proveedores de hardware también ofrecen tecnologías de desarrollo, como motores o SDKs propietarios, desempeñando así un doble papel como proveedores tanto de hardware como de tecnología para el desarrollo. Incluso pueden operar sus propios *storefronts* y lanzadores, como es el caso, por ejemplo, de los principales fabricantes de consolas.

Existen diferentes modelos y marcos que analizan las prácticas de la industria para identificar entre cuatro y siete etapas involucradas en el desarrollo de videojuegos. El ciclo de vida de los videojuegos o el proceso de *Game Development Software Engineering* (GDSE) suele ser diferente de las metodologías tradicionales de desarrollo de software debido a la diversidad inherente de requisitos introducidos por las disciplinas artísticas o creativas.

La mayoría de las conceptualizaciones del ciclo de vida de los videojuegos incluyen las tres fases principales, a alto nivel, resumidas en la Figura 2.

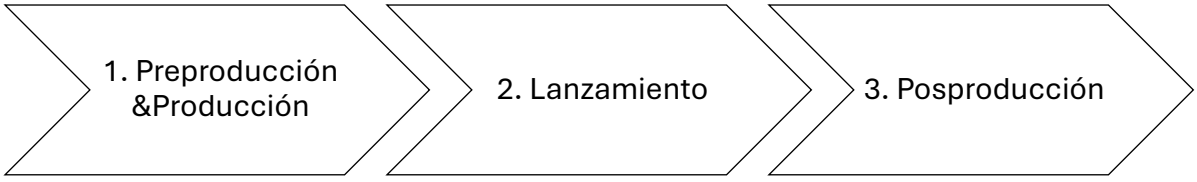

Figura 2. Ciclo de vida de los videojuegos

1. Preproducción y Producción

- Iniciación/Presentación/Concepto: Esta etapa marca la fase inicial donde se generan ideas y se describen conceptos y diseños preliminares. Implica definir las características principales del juego, como el género o las mecánicas centrales, para producir un concepto preliminar o un diseño de alto nivel.
- Preproducción: Esta etapa se centra en la planificación y preparación, y suele culminar con la creación de un documento de diseño detallado del juego. Las actividades incluyen la creación de *storyboards*, la construcción de prototipos y la confirmación de estructuras

internas. Normalmente termina con un prototipo jugable (o *vertical slice*[1]) que se utiliza para asegurar la financiación necesaria para completar la producción.

- Producción: Esta etapa se enfoca en la implementación de los conceptos del juego, detalles formales, refinamiento y desarrollo técnico y artístico (creación de recursos, código fuente, aspectos de integración). Suele ser la parte más larga del proceso.
- Pruebas: Esta etapa implica identificar y corregir errores, fallos, trampas y bloqueos. También se utiliza para probar la usabilidad, el factor de diversión y el compromiso del usuario con el juego. Los resultados de las pruebas ayudan a determinar si se debe proceder al lanzamiento o volver a la producción para realizar ajustes. Esta etapa suele ser concurrente: puede realizarse durante la producción desde las primeras fases de diseño, ya que los errores detectados más tarde son mucho más costosos de solucionar.
- Alpha/Beta/Prelanzamiento: Esta etapa implica poner el juego a disposición de probadores (internos o externos) para detectar errores y recopilar comentarios a mayor escala. La fase de prelanzamiento incluye las primeras campañas de marketing y de concienciación pública para avanzar hacia la siguiente fase.

2. Lanzamiento

Esta fase corresponde al lanzamiento público del juego. Incluye los retoques finales del juego, mejoras de calidad, los últimos retoques artísticos, la creación de la documentación adecuada y la planificación de actividades poslanzamiento.

3. Posproducción

Esta es la fase final, crucial para mantener la sostenibilidad. Las actividades incluyen la corrección de errores, la publicación de actualizaciones graduales, contenido descargable (*Downloadable Content* o DLC) y marketing. Los videojuegos se caracterizan por tener un ciclo de monetización largo, y la fase poslanzamiento fomenta la participación continua, ofreciendo visibilidad que puede derivar en ventas.

Debe tenerse en cuenta que este modelo de tres fases es adecuado para juegos tradicionales vendidos con un pago único, pero es menos aplicable a juegos *free-to-play* o *freemium*, donde la mayor parte del trabajo de producción (desarrollo) se realiza después del lanzamiento del producto. También cabe mencionar que los creadores, diseñadores y desarrolladores participan principalmente en la Fase 1, mientras que los editores y los *storefronts* tienen un papel fundamental en las Fases 2 y 3.

[1] Se trata de una sección pequeña y pulida del juego que muestra cómo será el producto final en términos de apariencia, sonido y jugabilidad. Incluye todas las capas principales de la experiencia de juego, pero solo para una parte limitada del mismo (escenario, sección, capítulo).

D. VIDEOJUEGOS Y EL RGPD

El sector de los videojuegos es una fuerza económica global fundamental en 2025, con unos ingresos anuales estimados que se acercan a los 200.000 millones de dólares. Esto lo sitúa por encima de las industrias del cine y la música. El sector sigue expandiéndose, impulsado por más de 3.000 millones de jugadores en todo el mundo y por la rápida innovación en áreas como el juego en la nube y la IA. Apoya cientos de miles de empleos, tanto directa como indirectamente, genera ingresos fiscales significativos y fomenta la innovación en tecnología, medios de comunicación y marketing a nivel global. Actualmente, el 95% de las ventas de juegos son digitales, lo que refleja el cambio generalizado hacia la distribución no física. Este cambio impulsa las plataformas y servicios en línea, y fomenta el desarrollo de nuevos modelos de negocio, como los basados en suscripción o en marketing digital.

A efectos del RGPD (Reglamento General de Protección de Datos)[2], los datos personales se definen como *"toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable 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"*; y el tratamiento se refiere a *"cualquier 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"*.

Por lo tanto, los videojuegos tratan datos personales, y todos los actores involucrados en la prestación de videojuegos deben cumplir con los principios y requisitos del RGPD al realizar actividades de tratamiento de datos que recaigan dentro del ámbito material y territorial de dicho reglamento.

El tratamiento de datos personales en los videojuegos va más allá de los registros tradicionales, como nombres o direcciones de correo electrónico; incluye cualquier información que diferencie a un jugador individual de otros en el contexto del juego, lo que permita realizar acciones dirigidas, interacciones personalizadas o tratamientos diferenciados. Este concepto de individualización activa las protecciones del RGPD, ya que permite que el juego trate a esa persona específica de manera única y diferenciada. Además, la toma de decisiones automatizada y la elaboración de perfiles se basan directamente en este concepto, ya que implican el uso de datos personales para analizar o predecir el comportamiento del jugador y, posteriormente, actuar sobre él de manera automática sin intervención humana.

Por este motivo es esencial proporcionar recomendaciones claras y específicas sobre cómo cumplir con el RGPD, ya que la industria de los videojuegos maneja grandes volúmenes de datos personales, a menudo muy sensibles. Esto se debe a que trata habitualmente información sobre usuarios vulnerables, como menores de edad, y también puede recoger o inferir categorías especiales de datos personales, como datos de salud, datos biométricos o cualquier otro dato que revele características sensibles. Además, el tratamiento realizado suele ser de alto riesgo, ya que implica no sólo datos sensibles a gran escala, sino también evaluaciones sistemáticas y exhaustivas, o la elaboración de perfiles y

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

la toma de decisiones automatizada, por mencionar solo algunos ejemplos. Por lo tanto, debido a su naturaleza, alcance, contexto o finalidad, es probable que genere amenazas significativas para los derechos y libertades de las personas.

Una orientación específica aclara las obligaciones, genera confianza entre las partes interesadas y aumenta la concienciación. Hay que tener en cuenta que los riesgos para la protección de datos comprometen la privacidad, la seguridad y, en general, los derechos y libertades de los usuarios. Además, esto puede socavar la estabilidad de las empresas a través de sanciones y daños reputacionales.

E. ALCANCE DE ESTE DOCUMENTO

Este documento recoge recomendaciones que facilitan el cumplimiento del RGPD específicamente dirigidas a profesionales y organizaciones del ecosistema de los videojuegos. Se centra en proponer medidas legales, organizativas y técnicas para el diseño, desarrollo y suministro de videojuegos de entretenimiento, y guiar a los equipos sobre cómo diseñar y ejecutar las actividades de tratamiento de datos personales dentro de sus títulos para que cumplan con los principios y requisitos del RGPD durante todo el ciclo de vida del juego.

II. TRATAMIENTO DE DATOS PERSONALES EN VIDEOJUEGOS

El tratamiento de datos personales en los videojuegos abarca numerosas actividades. Estas incluyen la recogida de datos personales para crear cuentas, la recopilación de telemetría sobre las acciones del jugador y sus sesiones de juego, y la realización de inferencias conductuales para la personalización y la monetización. Todas estas actividades tienen lugar dentro del complejo ecosistema de actores descrito previamente en este documento.

Los videojuegos tratan diferentes tipos de datos personales. Los identificadores directos están claramente vinculados a una persona conocida, como nombres de usuario, direcciones de correo electrónico, identificadores de cuenta o direcciones IP completas. Estos permiten a los editores contactar con personas específicas, iniciar sesión en un *storefront*, realizar transacciones financieras o que un jugador agregue a otro en una sala de juego. Además, hacen que funcionen las características principales, como guardar el progreso o seguir las clasificaciones.

Los pseudoidentificadores reemplazan esta información directa por sustitutos que, no obstante, individualizan a un jugador, como identificadores de dispositivo, identificadores publicitarios, *tokens* de sesión o combinaciones *hash* (por ejemplo, nombre de usuario + marca de tiempo). Un pseudoidentificador no puede atribuirse a una persona específica sin información adicional que se guarde por separado. En los juegos, por ejemplo, un UUID (*Universally Unique Identifier* o identificador único universal) que sigue a los jugadores en diferentes sesiones sin revelar su nombre u otros identificadores directos, lo que permite, por ejemplo, que los sistemas antitrampa o el botín personalizado se asocien a ese individuo específico en una partida multijugador.

Finalmente, los metadatos se refieren a datos que proporcionan información sobre otros datos o eventos dentro del entorno del juego. Describen atributos, actividades o sucesos, como marcas de tiempo, señales de geolocalización, registros de movimientos del ratón, datos de fallos o eventos dentro del juego (como muertes y compras), sin nombrar directamente ni distinguir explícitamente a los individuos. Sin embargo, los metadatos se convierten en datos personales cuando se vinculan a un contexto identificable. Por ejemplo, “Jugador en la IP 1.2.3.4 mató a un enemigo a las 14:32” combina metadatos con un identificador. Incluso los patrones de juego anonimizados (como un ritmo único de disparos de francotirador) pueden identificar a individuos cuando se analizan mediante *fingerprinting* conductual.

Esta sección describe las principales actividades de tratamiento, las categorías y elementos de datos relacionados, así como los fines más habituales. Todas las actividades de tratamiento consideradas implican el uso de identificadores, pseudoidentificadores y metadatos, además de datos de contenido y comunicación, datos financieros y transaccionales, datos de sensores, datos de localización, etc., como se abordará en el resto de esta sección.

A. CREACIÓN Y GESTIÓN DE CUENTAS

La creación de una cuenta, junto con los posteriores procesos de identificación y autenticación, representa una actividad fundamental de tratamiento de datos personales en los videojuegos. Este paso suele ser obligatorio para que los usuarios accedan a servicios clave, especialmente en juegos en línea y en *cloud/streaming*.

La creación de una cuenta implica la recogida directa y explícita de datos personales del usuario (el interesado) para crear una identidad digital persistente. En la fase inicial de registro, se recogen datos que pueden ser obligatorios u opcionales: la información esencial necesaria para establecer la identidad en línea del usuario y facilitar la seguridad (IAAA:

Identificación, Autenticación, Autorización y Auditoría), pero también para habilitar funcionalidades personalizadas. Además, los juegos suelen animar o recompensar a los jugadores por mantener su información de cuenta actualizada o completa, y por vincular sus cuentas con plataformas de redes sociales de terceros, lo que permite al juego acceder a datos personales adicionales regidos por la configuración de privacidad de la plataforma externa. La información asociada a las cuentas puede enriquecerse con el tiempo mediante inicios de sesión (o intentos) u otros aspectos relacionados con la seguridad. Todos estos datos pueden agruparse en varias categorías, que se muestran en la Tabla 2.

Categoría de datos	Elementos específicos
Datos básicos	Nombre y apellidos Dirección de correo electrónico Nombre de cuenta o de usuario Contraseña Número de teléfono Dirección postal
Datos demográficos	Edad o fecha de nacimiento Género País Idioma
Datos biométricos	Muestra de voz Imagen facial
Datos de terceras partes	Información sobre cuentas en redes sociales Listado de contactos o grafos sociales
Datos técnicos	Preferencias y configuración
Datos de pago	Número de tarjeta de débito o crédito Dirección de facturación Historial de compras
Datos de seguridad y protección	*Logs* de inicios de sesión *Tokens* de autenticación Marcadores de actividad sospechosa Historial de suspensiones Información asociada a los mecanismos antitrampa
Control parental	Registros de consentimiento parental Configuraciones para la limitación del juego Datos personales y de contacto de los padres o guardianes legales

Tabla 2. Datos personales tratados para la creación y gestión de cuentas

El tratamiento de datos personales para la creación y gestión de cuentas se realiza con varios fines, muchos de los cuales pueden ser necesarios para el cumplimiento de un contrato (es decir, permitir el juego y la prestación del servicio):

- Creación y acceso a la cuenta: Para crear cuentas de servicio y permitir a los usuarios acceder a él. El registro puede ser obligatorio u opcional en distintos niveles (*storefront*,

editor, proveedor de hardware) según el juego y sus características. Se anima encarecidamente a los usuarios a registrarse y convertirse en miembros, ya que, de lo contrario, podrían no poder acceder a funcionalidades o servicios clave.

- IAAA (Identificación, Autenticación, Autorización y Auditoría): Para verificar la identidad del usuario y proteger la seguridad de los servicios.
- Personalización y adaptación: Para crear perfiles de usuario y ofrecer contenido personalizado, lo que puede hacer que el juego sea más atractivo. La información de la cuenta puede ayudar a los distintos actores a comprender la demografía de los jugadores.
- Conexión con otros jugadores: Para establecer interacción social y conectar a los usuarios con otros jugadores en juegos multijugador en línea.
- Soporte al cliente y resolución de disputas: Para ofrecer soporte técnico, responder a las consultas de los usuarios, resolver disputas y hacer cumplir los acuerdos, términos y condiciones del servicio.
- Prevención del fraude y seguridad: Para realizar detección de actividad, prevenir transacciones fraudulentas (incluyendo el cumplimiento de los términos del servicio) y proteger a personas o grupos específicos.

B. MONITORIZACIÓN DEL JUEGO (TELEMETRÍA)

El tratamiento de datos personales en los videojuegos depende en gran medida de un tipo específico de monitorización, conocido como telemetría, que registra de manera continua el comportamiento y las métricas de rendimiento de los jugadores. Casi todas las pilas de tecnología de juegos modernos (dispositivos, tecnología de desarrollo, juego, lanzador) están diseñadas para transferir datos de comportamiento a servidores remotos a través de Internet. Esta actividad puede extenderse en el tiempo, registrando acciones, decisiones, comunicaciones, etc., generalmente con decenas de parámetros y señales capturadas por segundo.

Los videojuegos son entornos únicos, a veces considerados “laboratorios naturales y ricos de información”, donde el comportamiento de los jugadores puede activarse y monitorizarse intencionalmente bajo condiciones controladas, lo que hace que prácticamente todos los datos recogidos sean altamente sensibles. En este caso, la recogida de datos es implícita y pasiva, a menudo completamente invisible para el usuario normal. Los jugadores suelen desconocer la naturaleza y la cantidad de datos que se recogen y procesan sobre ellos.

Existen varios métodos extendidos para procesar la telemetría dentro de los juegos. El primer método se basa en integrar servicios de analítica de seguimiento de eventos. La mayoría de los juegos integran SDK de proveedores de analítica que permiten a los desarrolladores instrumentar eventos personalizados (por ejemplo, *«level_start»*, *«ability_used»*, *«shop_visit»*). Estos SDK agrupan la telemetría en paquetes pequeños y los envían de manera asíncrona a puntos de recogida externos, donde se almacenan en sistemas de almacenamiento de datos (*data warehouses*) para su análisis posterior.

El segundo método se basa en realizar registros en el lado del cliente y del servidor. Los juegos pueden registrar telemetría directamente en el cliente (registros JSON o binarios de sesiones, entradas o errores) y cargarlos periódicamente o en caso de fallo. La telemetría del lado del servidor suele ser más completa, ya que los servidores autorizados ven todos los estados, posiciones e interacciones de los jugadores sin posible manipulación del lado del cliente. Los títulos multijugador en línea suelen transmitir eventos estructurados (estilo

de juego, apariciones, muertes, indicadores de chat) a un *backend* de análisis centralizado, lo que permite paneles en tiempo real y la detección de fraudes o trampas.

El tercer método emplea APIs de telemetría remota y flujos UDP. En juegos de simulación o carreras, por ejemplo, los motores exponen datos de telemetría en tiempo real (posición, velocidad, tiempos por vuelta, estado del coche) a través de estas API o flujos con alta frecuencia. Herramientas de terceros (paneles, entrenadores de simulación de carreras, etc.) consumen este flujo a través de la red, tratando el juego como una fuente de telemetría que alimenta monitores externos, en lugar de limitarse solo al análisis interno al juego.

Por último, se puede utilizar muestreo e instrumentación basada en configuración remota. Algunos juegos utilizan estas estrategias para reducir el ancho de banda y el almacenamiento requeridos, registrando solo un subconjunto representativo de fotogramas o sesiones. La configuración remota permite a los desarrolladores activar o desactivar eventos específicos de manera remota, aumentar la profundidad de registro para ciertas regiones o segmentos de jugadores, o ajustar valores de parámetros sin necesidad de una actualización completa del juego, lo que es útil para pruebas A/B de jugabilidad o para la optimización de parámetros económicos.

Sin embargo, existen muchos otros métodos específicos para recoger y procesar este tipo de datos. Por ejemplo, mediante retroalimentación directa (preguntas, encuestas, sondeos) y PNJ (Personajes No Jugadores) o PNJ controlados por IA.

Los datos tratados con todos estos métodos diferentes se resumen en la Table 3.

Categoría de datos	**Elementos específicos**
Acciones en el juego	Duración, frecuencia, dirección, fuerza, velocidad o precisión de las acciones del jugador Acciones del personaje como movimiento/navegación, acciones de combate (disparar, dar patada, golpear, bloquear) o interacciones con objetos (coger, soltar, usar, abrir/cerrar)
Logros y progresión	Nivel en el juego Trofeos Clasificación Contenido desbloqueado
Estadísticas	Puntos, vidas, calificación Saldo de moneda en el juego Métricas de rendimiento, tasas de error, tiempo para completar tareas
Tiempo de juego	Conexiones (hora, duración) Frecuencia de juego Pausas, periodos de ausencia
Avatares	Perfil Características y modificaciones, *skins*
Logs y grabaciones	Acciones realizadas en los juegos y webs

	Archivos con grabaciones de los textos en los chats y las comunicaciones de voz Contenido generado por el usuario, entradas en foros
Datos biométricos	Características faciales, expresiones faciales y unidades de acción (por ejemplo, elevación de cejas) Dilatación de la pupila Patrones de movimiento ocular Posición de la cabeza Patrones de movimiento corporal Información y patrones relativos al cerebro Respuesta galvánica de la piel (*Galvanic Skin Response* o GSR) y sudoración Pulso cardíaco Respiración Tono y volumen de voz
Datos técnicos	Dirección IP Tipo y modelo de dispositivo, especificaciones del hardware Sistema operativo Calidad de la conexión Geolocalización

Tabla 3. Datos personales tratados para la monitorización del juego

El tratamiento de estos datos en el juego puede tener diferentes finalidades:

- Mejora del juego y optimización técnica: Los datos de telemetría se utilizan para mejorar la calidad del juego. Los desarrolladores analizan el comportamiento de los jugadores para perfeccionar las mecánicas del juego, identificando problemas como el nivel de dificultad de las fases, errores y problemas de usabilidad.
- Monetización y marketing: Los datos recogidos se utilizan para respaldar campañas de marketing dirigidas, lo que permite a los distintos actores del ecosistema determinar los momentos óptimos, el contenido y el público objetivo para la publicidad.
- Personalización y adaptación: Otra finalidad habitual es la personalización del juego. Los datos se utilizan para personalizar automáticamente el contenido y los servicios, adaptando las reglas y el contenido del juego al nivel de habilidad, las preferencias de jugabilidad o el estilo de juego del jugador. Esta finalidad suele implicar muy a menudo diferentes tipos de elaboración de perfiles.
- Prevención del fraude y seguridad: Los datos de telemetría pueden permitir la detección de comportamientos fraudulentos para mantener la integridad del juego, prevenir el fraude y hacer cumplir los términos del servicio.

C. INFERENCIAS DEL COMPORTAMIENTO

El tratamiento de datos personales en los videojuegos permite la generación de nueva información derivada del análisis de los datos recogidos directamente del usuario (principalmente, durante los procesos de creación y gestión de cuentas, pero también basándose en la retroalimentación recogida mediante encuestas y sondeos dentro del propio juego) y datos en bruto recogidos de manera pasiva (telemetría) generados durante el juego.

Como ya se ha discutido, la telemetría puede registrar entradas en bruto de hardware y dispositivos (como entradas de cámara y sensores multimodales, clics del ratón, pulsaciones de teclas, tiempos de presión de botones, derivas de *sticks*, presiones de gatillos, inclinación del dispositivo y respuestas de vibración). Además, se registran con marcas de tiempo precisas vectores de movimiento, muertes de personajes, finalizaciones de misiones, interacciones con objetos y duraciones de sesiones. La telemetría avanzada puede incluir mapas de calor que rastrean la mirada o los recorridos del cursor, o árboles de progresión que mapean las ramas de decisión. Al combinar toda esta información con otra, por ejemplo, relacionada con la creación y gestión de cuentas (registros de chat, uso de *emotes*, listas de amigos y formaciones de grupos, etc.) o incluso de fuentes externas, pueden producirse distintos tipos de inferencias sobre los jugadores.

La producción de inferencias es el proceso de analizar los datos recogidos en busca de patrones y relaciones estadísticas para derivar información personal adicional que el usuario no proporcionó de manera explícita o implícita. Este proceso implica la aplicación de métodos avanzados de análisis de datos, a menudo basándose en aprendizaje automático o inteligencia artificial.

Los flujos de datos en bruto alimentan la ingeniería de características, luego las CNN[3] analizan el tono de voz, volumen y disfluencias del habla para detectar excitación o frustración; las soluciones de NLP[4] y algoritmos de grafos clasifican roles sociales (líder, troll); el agrupamiento no supervisado (K-means/DBSCAN[5]) categoriza estilos de juego; los modelos supervisados (XGBoost[6], LSTM[7]) predicen el abandono/emoción a partir de series temporales; el aprendizaje por refuerzo adapta personajes no jugadores basándose en arquetipos inferidos como “triunfador” o “socializador”, el procesamiento en el borde en tiempo real permite la dificultad dinámica o generación de contenido, etc.

Los jugadores, de nuevo, con frecuencia desconocen la naturaleza y cantidad de sus datos recogidos y procesados. La Tabla 4 proporciona una visión general, no exhaustiva, de dichos datos.

Categoría de datos	Elementos específicos
Competencias y habilidades	Niveles inferidos en: • Pensamiento estratégico

[3] Las redes neuronales convolucionales (*Convolutional Neural Networks* o CNN) son redes de aprendizaje profundo diseñadas para procesar datos estructurados en forma de cuadrícula (como imágenes o flujos de telemetría en series temporales) y para aprender características jerárquicas mediante la optimización de filtros (o núcleos).

[4] Las soluciones de procesamiento de lenguaje natural (*Natural Language Processing* o NLP) tienen como objetivo que las máquinas comprendan, interpreten y generen lenguaje humano.

[5] K-means y DBSCAN (*Density-Based Spatial Clustering of Applications with Noise*) son algoritmos de aprendizaje automático de agrupamiento (*clustering*) no supervisado utilizados para agrupar puntos de datos basándose en similitud (e identificar valores atípicos como ruido).

[6] *Extreme Gradient Boosting* (XGBoost) es una biblioteca optimizada de código abierto diseñada para árboles de decisión de *gradient boosting* (GBDT) eficientes y escalables, ampliamente utilizada para clasificación, regresión y ranking.

[7] Las redes de memoria a largo y corto plazo (*Long-Short Term Memory* o LSTM) son un tipo específico de red neuronal recurrente (RNN) diseñadas para aprender dependencias a largo plazo en datos secuenciales, superando el problema de desvanecimiento del gradiente para modelar patrones temporales.

	• Reflejos • Precisión • Multitarea • Fluidez matemática • Trabajo en equipo • Memoria y retención
Emociones	Inferencias para detectar: • Estrés/relajación • Diversión • Frustración • Confianza • Decepción • Valencia de las emociones (reacciones positivas o negativas ante estímulos)
Rasgos de personalidad	Inferencias para evaluar: • Agresividad • Aversión al riesgo • Orientación a objetivos • Falta de fiabilidad • Tenacidad y determinación • Madurez psicológica global
Estatus económico y hábitos de consumo	Inferencias para determinar si el jugador es: • Frugal, responsable desde el punto de vista financiero • Derrochador • Impulsivo • Dispuesto a probar nuevos productos y servicios
Otras inferencias	Edad y género Medidas corporales e información biométrica Bagaje cultural Condiciones de salud mental y física Consumo de sustancias y drogas Procesos cognitivos

Tabla 4. Datos personales tratados para la inferencia de comportamiento

El tratamiento de estos datos puede tener diferentes finalidades:

- Mejora del juego y optimización técnica: El perfilado ayuda a analizar la dificultad de los niveles del juego, ajustar las mecánicas del juego y abordar problemas de usabilidad.
- Monetización y marketing: Se crean perfiles para predecir el comportamiento de compra, identificar usuarios financieramente excepcionales (a veces denominados “ballenas”, jugadores que gastan una gran, y poco habitual, cantidad de dinero en compras dentro del juego), y respaldar campañas de marketing dirigidas o de precisión. Diferentes

actores en el ecosistema pueden crear perfiles psicológicos basados en el juego, por ejemplo, para hacer que los jugadores pasen más tiempo conectados o compren contenido premium. Nuevamente, esta finalidad suele implicar el perfilado.

- Personalización y adaptación: Las inferencias se usan para personalizar automáticamente el contenido y los servicios según el nivel de habilidad, las preferencias de juego o el estilo de juego del jugador.
- Prevención del fraude y seguridad: Las inferencias pueden permitir la detección de comportamientos dañinos, la moderación de contenido, etc.

III. AMENAZAS Y RIESGOS PARA LA PROTECCIÓN DE DATOS

El tratamiento de datos personales en los videojuegos plantea amenazas y riesgos específicos más allá de los que se presentan en entornos de tecnologías de la información tradicionales, impulsados por la telemetría generalizada, el perfilado conductual y modelos de monetización cada vez más sofisticados. Esta sección identifica las principales amenazas para la protección de datos en el ecosistema de los videojuegos mediante la metodología LIINE4DU[8], y analiza su posible impacto en los derechos y libertades de los interesados, como base para ofrecer recomendaciones y buenas prácticas más adelante en este documento.

A. VINCULACIÓN

Esta amenaza implica asociar diferentes elementos de datos o acciones del interesado para obtener más información sobre el interesado o el grupo al que pertenece. Los jugadores pueden vincularse a sus transacciones y actividades a través de diferentes pseudoidentificadores recogidos de manera explícita o implícita.

Los editores de juegos en línea y los *storefronts* pueden utilizar tecnologías como *cookies*, web *beacons*, etiquetas o *fingerprinting* de dispositivo/navegador para rastrear a usuarios individuales y sus actividades en diferentes sesiones de juego, incluso cuando no han iniciado sesión.

El rastreo entre juegos a menudo es posible simplemente a partir del nombre de usuario de un jugador, que puede ser el mismo en diferentes juegos y plataformas. Otra forma de rastreo se basa en el uso de las características únicas de un interesado, como la forma en que maneja las interfaces (teclado, ratón, mando, etc.) o su estilo de juego individual (por ejemplo, una secuencia específica de acciones en juegos de estrategia o un perfil de conducción en juegos de carreras).

Además, los datos de los jugadores rara vez se limitan a los servidores internos del editor del juego o del *storefront*. Con frecuencia, se combinan con fuentes de datos externas. Estos actores suelen compartir los datos de los usuarios con diversas terceras partes, como redes de juegos, corredores de datos, proveedores de *middleware* y analítica, y plataformas publicitarias. La información compartida puede luego asociarse con datos de terceros sobre el mismo usuario.

Debe considerarse que los juegos suelen instar a los usuarios a vincular sus cuentas de redes sociales, lo que aumenta aún más el riesgo de que se materialicen las amenazas de vinculación. Además, jugar en dispositivos externos, como teléfonos móviles, introduce formas adicionales de recoger datos y combinar la información del juego con conjuntos de datos de terceros.

La extensa recopilación de datos vinculables puede alimentar métodos avanzados de elaboración de perfiles, a menudo basados en inteligencia artificial, que vinculan datos en bruto con rasgos personales sensibles: habilidades y capacidades, emociones, situación financiera, vulnerabilidad al diseño adictivo, etc., utilizados por diferentes partes para predecir e influir en el comportamiento futuro de los usuarios. Esto puede dar lugar a explotación y manipulación (desde aumentar el efecto manipulador de la publicidad dirigida hasta influir en opiniones políticas o hacer que los jugadores pasen más tiempo en el juego y alimentar o fomentar tendencias adictivas). La vinculación puede usarse para perfilado de usuarios como “propensos a gastar” o “ballenas”, con el objetivo de inducirlos a gastar sumas exorbitantes de dinero real dentro del juego.

[8] An introduction to LIINE4DU 1.0: A new privacy&data protection threat modelling framework, https://www.aepd.es/guides/technical-note-introduction-to-liine4du-1-0.pdf

La discriminación dentro y fuera del ecosistema de los videojuegos (dadas las prácticas de compartición de datos) también puede ser un impacto. Por ejemplo, los datos vinculables y las inferencias pueden usarse para calcular un factor de riesgo financiero a partir del comportamiento en el juego, lo que potencialmente podría llevar a que se le deniegue un préstamo o una ampliación de línea de crédito a un usuario. Inferencias similares también podrían usarse para evaluar las cualidades esenciales de un jugador y determinar su idoneidad para ciertos empleos.

B. IDENTIFICACIÓN Y *DOXING*

La identificación implica que uno de los actores del ecosistema de los videojuegos conozca la identidad de un interesado de manera directa (por ejemplo, mediante el tratamiento de información identificable o brechas de datos) o indirecta (por ejemplo, mediante deducción o inferencia).

Registrarse con los actores del ecosistema para acceder a los últimos juegos y funcionalidades suele requerir proporcionar datos de identidad del mundo real. Esto hace que la amenaza se materialice casi de inmediato, ya que los datos de registro suelen incluir información de identificación personal, como nombre completo, dirección de correo electrónico, dirección postal y datos de la tarjeta de crédito.

Esto se agrava con la amenaza de vinculación, ya que, en muchos casos, solo un actor del ecosistema conoce la identidad del jugador, pero, mediante la vinculación y el perfilado, otros pueden llegar a conocerla también.

Incluso cuando un jugador no revela su identidad real, la integración con cuentas de redes sociales o el uso de teléfonos móviles puede revelarla. Además, al personalizar personajes y perfiles (por ejemplo, mediante el nombre de usuario, la edad, el idioma o el género), los jugadores pueden revelar sin querer aspectos sobre sí mismos, contribuyendo a la identificación. Asimismo, los dispositivos de juego modernos suelen recoger datos biométricos (voz, rasgos faciales, movimientos, tamaño corporal y patrones oculares), que por sí solos podrían ser suficientes para permitir la identificación del jugador.

La amenaza de identificación a menudo se combina con rasgos conductuales y psicológicos inferidos. Como resultado, el ecosistema de los videojuegos puede ser una herramienta poderosa para la vigilancia digital, lo que hace que los jugadores sean vulnerables a la explotación externa y al uso inesperado de sus datos.

El *doxing* es, esencialmente, la difusión pública de información privada sobre una persona (como su nombre real, dirección particular o datos laborales), que la persona pretendía mantener confidencial. Cuando la identidad real de un jugador se difunde públicamente, ya sea por malicia intencional (acoso por parte de otro jugador) o por una brecha de datos, la amenaza de identificación se materializa como un caso de *doxing*.

Las jugadoras, en particular, pueden sufrir el riesgo de acoso y suelen adoptar estrategias como ocultar su género gestionando cuidadosamente su perfil/personaje en el juego o evitando los chats de voz para alejar a los acosadores. Si se difunde públicamente información identificable precisa, como datos de ubicación, las consecuencias del *doxing* van más allá del ámbito digital y pueden comprometer su seguridad física.

C. INEXACTITUD

Las amenazas de inexactitud en los videojuegos surgen cuando los datos personales (incluidos los datos de telemetría en bruto y las inferencias) son incompletos, obsoletos o incorrectos en relación con la finalidad del tratamiento.

Si los datos de un jugador, incluidos los intentos de inicio de sesión y los aspectos relacionados con la seguridad, no se mantienen actualizados de manera continua, pueden volverse obsoletos y afectar a la gestión y la seguridad de la cuenta. Más concretamente, los juegos suelen especificar límites de edad (por ejemplo, +13 o +18) y se basan en la prueba de edad proporcionada durante el registro. Si el proceso de verificación de edad no es fiable ni lo suficientemente robusto, y se utiliza un perfil de edad obsoleto o incorrecto, esto puede impedir el acceso legítimo de adultos o permitir el acceso de menores no autorizados, con las consiguientes implicaciones para su protección.

Los datos de telemetría suelen usarse para personalizar el contenido y los servicios del juego según los estilos y preferencias de juego individuales. Si estos datos son inexactos, las experiencias personalizadas pueden volverse irrelevantes o incompatibles, afectando negativamente a la experiencia de juego y reduciendo, por tanto, la satisfacción del jugador.

Los datos de telemetría también son esenciales para mantener la integridad de los juegos en línea, en particular para detectar trampas. Si los datos de telemetría utilizados para la detección son inexactos o se interpretan incorrectamente, un jugador legítimo podría ser marcado erróneamente por comportamiento deshonesto, lo que podría dar lugar a consecuencias injustas como la suspensión o el bloqueo. Además, si los fallos en el sistema impiden la detección precisa de tramposos, los tramposos genuinos podrán seguir haciendo trampa. Esto, a su vez, otorga ventajas injustas y perjudica la experiencia de juego de los jugadores honestos. Asimismo, los tramposos que usan *bots* o *hacks* pueden aumentar la oferta de bienes virtuales, lo que devalúa los productos obtenidos por los jugadores legítimos, y lleva a una pérdida de beneficios para esos jugadores en particular, así como a una distorsión de las economías dentro del juego en general.

Como se mencionó antes, las empresas de videojuegos utilizan métodos avanzados de análisis de datos para extraer patrones y relaciones estadísticas de los datos de juego, generando información personal derivada que el usuario no ha proporcionado de manera explícita. Si los datos en bruto contienen ruido, son incompletos o están corruptos (por ejemplo, debido a problemas de conectividad, retrasos del servidor o errores de software) o los mecanismos de inferencia presentan fallos, las inferencias conductuales derivadas serán inexactas, pero se estarán usando para la toma de decisiones automatizada. Por ejemplo, una evaluación automatizada de “sigilo” realizada dentro del entorno del juego intenta medir la competencia en habilidades como el pensamiento estratégico, las habilidades motoras finas o la memoria. Si los datos en bruto subyacentes son defectuosos, la evaluación de las habilidades del jugador podría ser inexacta, lo que podría llevar a una clasificación errónea de sus competencias, lagunas de conocimiento o dificultades de aprendizaje, afectando, en consecuencia, su experiencia de juego de manera negativa.

Como se mencionó antes, los datos de juego pueden analizarse para calcular un factor de riesgo financiero, que luego puede compartirse con terceros, como aseguradoras o empleadores. Si los datos de telemetría subyacentes (que pueden indicar si un usuario es ahorrador, responsable desde el punto de vista financiero o derrochador) o el resultado de los sistemas de inferencia son inexactos, un jugador podría enfrentar discriminación en el mundo real, como la denegación injusta de un préstamo o un empleo, basada en una evaluación errónea derivada de sus actividades virtuales.

Las inexactitudes también pueden materializarse en la información compartida con otros usuarios o con el público, afectando a la experiencia social y a la reputación del jugador. Las

funcionalidades sociales permiten que otros jugadores vean el nombre de usuario, el avatar y el progreso en el juego de un jugador, así como información relacionada con el juego, como las puntuaciones más altas. Si los datos de progreso subyacentes son inexactos (por ejemplo, debido a trampas no detectadas o a errores en el juego que afectan a las métricas), la representación del jugador ante sus compañeros será errónea, lo que podría afectar a su posición social o a la equidad de los emparejamientos que se realicen.

D. NO REPUDIO

Las acciones de los jugadores y su actividad en el juego se registran, almacenan y conservan de manera persistente. Este registro sienta las bases para las amenazas de no repudio: un interesado no puede negar su participación en acciones, como comunicarse con otros jugadores, ser sospechoso de hacer trampa o realizar una transacción financiera:

- Los juegos en línea, en particular aquellos con modos multijugador, suelen registrar y almacenar las comunicaciones entre jugadores (como el texto del chat y los datos de voz). Esta monitorización suele tener como objetivo proteger a los usuarios mediante la identificación en conversaciones de lenguaje ofensivo e interacciones abusivas.
- La monitorización del juego (telemetría) registra de manera continua el comportamiento, el rendimiento, las acciones y las decisiones del jugador. El análisis de estos datos de alta granularidad puede descubrir trampas y otras prácticas desleales, atribuir estos comportamientos a jugadores específicos y hacer cumplir las normas de juego limpio.
- Cuando se intercambia dinero real por contenido dentro del juego, es necesario un registro absoluto para establecer responsabilidades y prevenir el fraude financiero.

Todos estos mecanismos, y otros similares crean una cadena sólida de pruebas que permite al ecosistema mostrar de manera definitiva quién realizó qué acciones. En algunos casos, estas pruebas son un requisito legal o esencial para la seguridad y las funcionalidades principales. Sin embargo, estos sistemas también eliminan la capacidad del jugador de negar de manera plausible cualquier acción, ya sea positiva (como completar desafíos o niveles del juego) o negativa (como jugar videojuegos muy violentos con gran frecuencia, acosar a otros o hacer trampas), incluso cuando no existe una obligación legal de conservar un registro o cuando no es estrictamente necesario para prestar el servicio principal. El principal impacto de los mecanismos de no repudio es la falta de negación plausible, lo que puede dar lugar a consecuencias sociales y legales dentro y fuera del entorno del juego.

Si se determina que un jugador ha incumplido los términos (abuso, fraude), por ejemplo, los registros que justifican la decisión de aplicar una sanción como un bloqueo permanente pueden conservarse indefinidamente. Estos registros pueden impedir que el jugador cree una nueva cuenta no sancionada en el mismo juego o plataforma, o en uno diferente, ahora o en el futuro. Fuera del ecosistema de los videojuegos, un empleado podría ser despedido porque los registros detallados de telemetría sobre el tiempo que pasó jugando se comparten con su empleador, proporcionando así pruebas irrefutables y con marca de tiempo utilizadas en una terminación laboral formal: el empleado estaba jugando durante su horario de trabajo y no puede negarlo.

Asimismo, como el no repudio suele basarse en algoritmos complejos y propietarios, los jugadores que deseen impugnar una decisión automatizada (por ejemplo, una sanción por trampa que es injusta o equivocada) podrían encontrar dificultades significativas al intentar hacerlo. El sistema tiene las pruebas de la acción, incluso si el jugador argumenta que la acción fue involuntaria o identificada erróneamente por el algoritmo. El posible impacto de

una combinación con una amenaza de inexactitud o una amenaza de no intervención (para oponerse a ser objeto de una decisión automatizada) debe ser analizado.

E. BRECHA DE DATOS

Las brechas de datos representan una amenaza crítica para el ecosistema de los videojuegos, ya que incidentes importantes han expuesto cantidades significativas de información de los jugadores recogida y tratada por las empresas del sector en el pasado. Con un número de jugadores en línea que ha superado los 1.300 millones en todo el mundo en 2025, el alcance potencial de estas brechas es enorme.

Una brecha de datos es una violación de la seguridad de los datos personales que ocasiona la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Los datos personales de los jugadores, como nombres, contraseñas, direcciones de correo electrónico, números de teléfono e incluso datos financieros, pueden verse comprometidos. Esta información puede venderse o usarse para lanzar nuevos ataques, lo que aumenta considerablemente el riesgo de robo de identidad o fraude y lleva a consecuencias más amplias, como compras o préstamos ilegales realizados con los datos robados.

La exposición de credenciales en las brechas de datos suele propiciar la suplantación de cuentas, lo que puede dar lugar, por ejemplo, a la pérdida de activos y moneda dentro del juego. Cuando los jugadores reutilizan contraseñas en varias cuentas, una única brecha permite a los adversarios acceder a múltiples cuentas de juegos o incluso a cuentas más sensibles, un escenario conocido como *credential stuffing*.

Dado que la industria también trata grandes cantidades de datos de telemetría e inferencias a partir de datos conductuales, la divulgación no autorizada podría exponer información íntima sobre las habilidades, emociones y rasgos de personalidad de un usuario, así como sus comunicaciones dentro del juego, indicadores de trampa y otra información sensible.

F. ENGAÑO

Los patrones oscuros, también conocidos como diseños engañosos, amenazan a los jugadores mediante el uso de interfaces de usuario manipulativas, motivadas principalmente por la monetización. Estos diseños influyen en el comportamiento de los jugadores, lo que a menudo lleva a la divulgación no intencionada de datos personales o a pérdidas económicas al aumentar la probabilidad de que los jugadores compartan datos personales o gasten dinero.

Los patrones de diseño engañoso utilizan técnicas manipulativas específicas para engañar a los jugadores y llevarlos a tomar decisiones que de otro modo evitarían. Estas técnicas explotan vulnerabilidades psicológicas y sesgos cognitivos mediante la variación intencional de emociones, colores, lenguaje, opciones, etc.

Por ejemplo, algunos juegos facilitan el registro con cuentas de redes sociales en comparación con el registro con una dirección de correo electrónico. Otros juegos ofrecen recompensas dentro del juego para animar a los jugadores a vincular sus cuentas de redes sociales o a compartir listas de contactos. Los patrones oscuros también pueden presionar a los jugadores para que se suscriban o hagan clic en anuncios. A menudo, un juego afirma que cancelar antes de que termine el período de prueba gratuito es fácil, cuando en realidad

es difícil. Otros patrones fomentan las microtransacciones, las cajas botín o los mecanismos de pago para ganar, aumentando así la presión para gastar dinero dentro del juego.

En general, los patrones oscuros se utilizan para animar y recompensar activamente a los jugadores por actividades que pueden tener impactos negativos para ellos, pero a menudo no reciben información clara sobre estas consecuencias negativas de sus decisiones, que también pueden estar muy guiadas, incitadas o influenciadas.

Los patrones adictivos forman un subconjunto de los patrones engañosos. Son prácticas de diseño destinadas a animar a los usuarios a pasar mucho más tiempo en plataformas digitales o a comprometerse más profundamente de lo que es saludable o esperable. El principal riesgo del diseño adictivo es el uso excesivo y compulsivo de productos digitales, como los videojuegos. Las consecuencias negativas incluyen la pérdida de tiempo (los usuarios pasan conectados mucho más tiempo del previsto) y el daño psicológico (que puede contribuir a problemas de salud mental). Cabe destacar que el "trastorno por uso de videojuegos" está reconocido como una condición médica en la Clasificación Internacional de Enfermedades (CIE-11) de la OMS, en vigor desde 2022.

Patrones adictivos como jugar por cita, el *grinding* y la mera exposición, las recompensas periódicas o la presión social y la comparación se utilizan con frecuencia en el diseño de videojuegos. Dado que los actores que participan en el ecosistema poseen grandes cantidades de información sobre los jugadores, esta asimetría informativa puede usarse para manipular su comportamiento, lo que dificulta que los usuarios comprendan cómo están siendo influidos y se protejan. Cuando un jugador invierte más tiempo en un juego, el ecosistema del juego recoge un mayor volumen y variedad de datos conductuales de alta dimensionalidad. Cuanto más largo sea el tiempo de juego y mayor el conjunto de datos recogidos, más fácil resulta para los desarrolladores y las plataformas aplicar métodos avanzados de análisis de datos para descubrir patrones e inferir información personal sensible que el usuario nunca proporcionó de manera explícita. Este proceso transforma los datos en bruto en conocimientos profundos que posibilitan la toma de decisiones sobre el jugador. Este conocimiento adquirido orienta el despliegue preciso de patrones de diseño engañosos y adictivos para maximizar el intercambio de datos, la generación de ingresos, el compromiso y la fidelización.

G. DIVULGACIÓN

La amenaza de divulgación de datos en los videojuegos implica la recogida, el almacenamiento, el procesamiento o la compartición/transferencia de datos personales más allá de lo que los jugadores anticipan, esperan o consienten.

Los videojuegos en línea modernos pueden recopilar enormes cantidades de datos de usuario de alta dimensionalidad y muy detallados, que a menudo superan lo necesario para la jugabilidad principal. La sección anterior de este documento ha presentado los tipos de datos personales que los juegos suelen tratar, como los datos para la creación y gestión de cuentas, la telemetría y la inferencia conductual. Esta sección también ha tratado, en relación con otras amenazas, la capacidad de inferir datos personales sensibles, como puntuaciones de riesgo financiero.

En las amenazas de divulgación de datos, debe hacerse una distinción clave entre los datos que los jugadores proporcionan de manera explícita y aquellos que se recogen o infieren de manera implícita (a través de telemetría o análisis conductual). Estas categorías difieren en el grado de conocimiento de los usuarios y en los tipos de información revelada.

Los datos proporcionados de manera explícita incluyen la información que los usuarios introducen ellos mismos (nombre, correo electrónico, edad, género, número de teléfono,

datos bancarios) durante el registro o las transacciones. Los jugadores saben que están compartiendo esta información y pueden adaptar su comportamiento en consecuencia. Por ejemplo, podrían protegerse utilizando perfiles falsos. En cambio, los datos de telemetría y los datos inferidos se recogen automáticamente a partir de acciones dentro del juego, el uso de dispositivos o sensores, a menudo sin que el usuario sea consciente de ello. Los juegos analizan estos datos en bruto para inferir información sensible que los usuarios no han proporcionado intencionalmente. Dado que los jugadores normalmente no son conscientes de la magnitud de esta recolección de datos ni de las inferencias que se extraen de ellos, tienen poco control sobre la información sensible divulgada.

La recogida implícita de datos amplía considerablemente el alcance de la información expuesta. Como ya se ha mencionado, los datos del juego y de los sensores pueden revelar mucho más que la información demográfica por sí sola. Por ejemplo, pueden revelarse emociones, habilidades, intereses, hábitos, rasgos de personalidad, estado socioeconómico y aspectos de la salud física o mental. Métodos de recogida como el software antitrampas del lado del cliente o los sensores integrados (cámaras, micrófonos, seguimiento ocular) pueden acceder de manera intrusiva al dispositivo de un usuario o incluso a su cuerpo.

Debe considerarse que los dispositivos de juego utilizan cada vez más sensores para recoger datos altamente sensibles, como la voz, los gestos y las expresiones faciales. Por ejemplo, los auriculares de realidad aumentada/realidad virtual (RA/RV) capturan datos biométricos como la postura, los movimientos oculares, la conductancia de la piel y la frecuencia cardíaca, lo que permite inferir información altamente sensible.

Actualmente, se están introduciendo en el ecosistema de los videojuegos auriculares de electroencefalograma (EEG) no invasivos, a menudo denominados interfaces cerebro-computadora (*Brain Computer Interace* o BCI). Estos dispositivos miden la actividad eléctrica en el cerebro mediante sensores en el cuero cabelludo. Luego, el software filtra el ruido y aplica modelos de aprendizaje automático o inteligencia artificial para mapear patrones específicos de ondas cerebrales o estados mentales (como “concentración” o “relajación”) a comandos dentro del juego, como moverse, saltar o activar una habilidad. Existen dos paradigmas principales en uso. El primero, llamado BCI activo o de comando mental, requiere que los jugadores entrenen al sistema para asociar una acción imaginada específica o una estrategia mental con un comando específico del juego (por ejemplo, pensar “empujar” para mover un objeto). El segundo, denominado sistemas pasivos o neuroadaptativos, supervisa de manera continua los estados cognitivos o emocionales (como el compromiso, el estrés o la fatiga) para adaptar la dificultad, el ritmo o el contenido del juego sin que el jugador tenga que emitir comandos mentales deliberados. El *neurogaming* recoge y procesa constantemente neurodatos que pueden revelar información sobre los estados mentales, las emociones y otros rasgos sensibles de los jugadores.

Los sensores modernos también pueden monitorizar la posición y el entorno de un usuario, e incluso captar datos sobre personas cercanas. Los juegos también pueden solicitar acceso a datos de otras aplicaciones en el mismo dispositivo o de las redes sociales del usuario, como contactos, documentos, correos electrónicos y archivos.

Las amenazas de divulgación de datos suelen culminar en la amplia distribución de la información de los jugadores a terceros, afiliados u otros jugadores. Las empresas de videojuegos comparten regularmente los datos de los jugadores con otros actores como anunciantes, socios, redes de juegos, proveedores de *middleware*, proveedores de analítica y agregadores. Dado que los juegos operan a nivel mundial, los datos pueden transferirse a países con marcos regulatorios para la protección de datos menos robustos que las del país del jugador.

H. DESCONOCIMIENTO Y FALTA DE CAPACIDAD PARA INTERVENIR

Esta amenaza implica no demostrar de manera suficiente el cumplimiento o no informar, involucrar o facultar de manera suficiente a los interesados en el tratamiento de sus datos personales.

Los videojuegos son servicios digitales complejos que, muy a menudo, utilizan mecanismos avanzados de inferencia, perfilado e incluso vigilancia. Estas características pueden estar profundamente integradas en el entorno del juego, funcionando de maneras que no son visibles u obvias para los jugadores.

Los juegos recogen una enorme cantidad de datos detallados de los usuarios, que los jugadores comunes no pueden rastrear fácilmente. Los jugadores suelen desconocer tanto el tipo como la cantidad de datos recogidos, así como la forma en que se utilizarán. Las técnicas avanzadas de análisis de datos extraen inferencias personales a partir de patrones ocultos en el juego o en los datos recogidos por los sensores, lo que dificulta que los usuarios anticipen estas actividades. Además, muchos jugadores no son conscientes de que las comunicaciones dentro del juego (como los chats de voz) pueden ser monitorizadas, grabadas o compartidas con terceros. La naturaleza inmersiva y ficticia de los videojuegos puede distraer a los jugadores de riesgos reales para la privacidad, creando una falsa sensación de anonimato que podría fomentar un comportamiento más arriesgado, que revele más datos personales o más sensibles.

Aunque las normativas exigen un alto grado de transparencia, la mayoría de los juegos se basan principalmente en las políticas de privacidad como su principal medio para informar a los jugadores. Estos documentos suelen ser extensos, densos y llenos de jerga legal, lo que a menudo los hace difíciles de entender. Como resultado, muchos usuarios los omiten y comienzan a jugar de inmediato. Las políticas suelen utilizar redacciones vagas, como “mejorar la experiencia del usuario” como finalidad para las actividades de tratamiento de inferencias conductuales, “respaldar los servicios publicitarios” como finalidad para el perfilado y el intercambio de datos de los jugadores con terceros, u “ofrecer funcionalidades personalizadas” para describir cómo se recogen y utilizan los datos. Esta falta de detalle no logra explicar la base legal para el tratamiento de datos personales en primer lugar.

En cuanto a la falta de capacidad para intervenir, surge cuando los jugadores, incluso si son conscientes de los riesgos que corren, carecen de formas simples y efectivas para controlar sus datos. Esto hace que la intervención activa o la toma de decisiones sobre su privacidad sea difícil o imposible.

Por ejemplo, muchos juegos no proporcionan controles accesibles o valiosos para gestionar los datos personales, en contra de las expectativas de los jugadores. Incluso cuando existen configuraciones de privacidad, rara vez están centralizadas y suelen ser difíciles de encontrar e interpretar, lo que deja a los jugadores confundidos sobre sus opciones y, a veces, efectivamente obligados a aceptar configuraciones invasivas para la privacidad (como permitir el seguimiento) para acceder a todas las funcionalidades del juego.

Los jugadores deberían poder ejercer sus derechos, por ejemplo, para acceder, corregir y eliminar fácilmente sus datos. Sin embargo, las configuraciones o políticas de privacidad excesivamente complejas o extensas dificultan la gestión de sus datos personales. Además, la revocación del consentimiento debería ser tan simple como otorgarlo en primer lugar.

I. AMENAZAS PARA LA INFANCIA Y OTROS JUGADORES VULNERABLES

El ecosistema de los videojuegos plantea amenazas agravadas para la infancia y otros jugadores vulnerables debido a la combinación de su etapa de desarrollo, su alto nivel de participación, su limitada alfabetización digital y el foco de la industria en la recogida de sus datos y la monetización. Aunque todos los jugadores enfrentan los mismos riesgos, la infancia y otros grupos vulnerables suelen estar menos capacitados para reconocer o mitigar su impacto y son más susceptibles a la manipulación.

Las niñas, niños y adolescentes (NNA), como clase vulnerable de interesados, requieren una protección reforzada en línea debido a su limitada conciencia de los riesgos del tratamiento de datos, especialmente en entornos digitales como los videojuegos. El RGPD exige que las empresas verifiquen de manera razonable la autorización de los padres o tutores al tratar los datos de menores sobre la base del consentimiento, especialmente para aquellos menores de 16 años (o una edad inferior, según la establezcan los Estados Miembros).

Los NNA constituyen una parte significativa de los jugadores y son objeto frecuente de marketing. Pueden tener predisposición a intercambiar datos personales a cambio de incentivos. A menudo, carecen de conciencia sobre la configuración de privacidad y rara vez toman precauciones de privacidad en línea. Muchos no reconocen qué datos se recogen ni los fines para los que se tratan.

Pueden ser engañados o explotados por especialistas en marketing en línea que utilizan técnicas específicas y anuncios dinámicos adaptados a sus perfiles y patrones de comportamiento. La recogida de datos, que a menudo se produce a través de mecanismos implícitos, puede dar lugar a que sean tratados como conjuntos algorítmicos. Esto puede limitar su diversidad, su potencial y sus oportunidades. Los riesgos resultantes incluyen el robo de identidad, la pérdida de reputación y la discriminación tanto actual como futura, e incluso la estigmatización.

Las interacciones en línea pueden exponer a los jugadores vulnerables al acoso, la discriminación y el *bullying* si se comparten atributos de identidad personal. La divulgación de raza, género, orientación sexual o ideas políticas puede dar lugar a abusos. Los entornos de juego suelen reflejar las hostilidades sociales, y las minorías enfrentan comportamientos inapropiados. La edad, la religión, la nacionalidad o las habilidades en el juego también pueden convertir a las personas en objetivos. Los NNA, que aún están desarrollando habilidades sociales, están especialmente en riesgo y requieren protección adicional. Además, los actores malintencionados explotan las herramientas de comunicación dentro del juego, como los chats de voz y texto, para difundir narrativas de odio, extremistas y desinformación, afectando a miles de personas, incluidos menores.

Existen riesgos de explotación, como hacer trampa para obtener recompensas o robar activos virtuales. La suplantación de identidad también es una preocupación, como cuando un jugador finge ser una autoridad para recopilar datos sensibles. Estos riesgos pueden tener consecuencias graves más allá del juego, como el fraude de identidad y problemas de geolocalización que pueden afectar a la seguridad y la integridad física.

El auge de los modelos *free-to-play* (F2P) y las microtransacciones expone a los NNA a presiones comerciales para las que pueden no estar preparados. Las preocupaciones en torno a la monetización incluyen la posibilidad de que el juego domine la vida diaria (comportamientos adictivos) y el riesgo de pagar de más. Los NNA especialmente los más pequeños, pueden ser menos resilientes a la presión del marketing o menos conscientes el valor de los productos, en particular cuando las plataformas permiten la compra rápida y sencilla de artículos dentro del juego. El diseño engañoso puede explotar vulnerabilidades creando la impresión de que los jugadores que no realizan compras dentro del juego

perderán contenido exclusivo o ventajas de juego. Esta inseguridad social relacionada con quedarse atrás respecto a otros jugadores que gastan dinero puede fomentar compras impulsivas o adicción al juego. Lo mismo ocurre con las ofertas limitadas en el tiempo o de una sola vez dirigidas a NNA. Además, las recompensas aleatorias, como las cajas botín, plantean riesgos específicos para estos jugadores vulnerables.

Las siguientes secciones ofrecen recomendaciones y buenas prácticas para ayudar a los responsables y encargados del tratamiento en el ecosistema de los videojuegos a cumplir con las obligaciones principales del RGPD, incluidos los principios del Artículo 5 (licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, responsabilidad proactiva); las bases jurídicas y condiciones especiales de los Artículos 6, 8 y 9; los derechos de los interesados (incluidas las salvaguardias frente a decisiones individuales automatizadas del Artículo 22); la protección de datos desde el diseño y por defecto (Artículo 25) y la seguridad del tratamiento (Artículo 32). Las recomendaciones proporcionadas ayudan a evitar o mitigar amenazas como las identificadas en la sección III de este documento. No son un resumen de recomendaciones genéricas ya conocidas para cumplir con los principios y obligaciones de protección de datos del RGPD, sino recomendaciones específicas sobre aspectos concretos presentes en los videojuegos.

Aunque estas medidas específicas ofrecen una vía práctica de cumplimiento adaptada a cada etapa del ciclo de vida y actividad de tratamiento, los actores del sector siguen siendo libres de identificar e implementar enfoques alternativos que satisfagan igualmente estos requisitos. Cualquier desviación debe documentarse con una justificación clara que demuestre niveles de protección equivalentes, y debe garantizarse la plena responsabilidad por el diseño o la implementación elegidos.

IV. RECOMENDACIONES Y MEJORES PRÁCTICAS EN LA FASE DE PREPRODUCCIÓN Y PRODUCCIÓN

La preproducción es la fase en la que comienza a formarse la identidad conceptual, narrativa y técnica de un videojuego. También es la fase en la que se determina la postura de cumplimiento a largo plazo del responsable del tratamiento. Para cuando un juego llega a su lanzamiento, muchas de las decisiones importantes en relación con el cumplimiento del RGPD, como la necesidad y proporcionalidad de determinadas actividades de tratamiento de datos, los fines que pueden perseguirse legítimamente, las categorías de datos personales recogidos y la arquitectura de la protección de datos desde el diseño, ya están integradas en la estructura del juego. Por esta razón, los principios fundamentales del RGPD, como la licitud, la lealtad, la transparencia, la limitación de la finalidad, la minimización de datos y la protección de datos desde el diseño y por defecto, deben orientar las decisiones creativas y técnicas iniciales en lugar de funcionar como restricciones añadidas posteriormente en el ciclo de vida. El cumplimiento no solo es compatible con el diseño innovador de juegos, sino que también puede mejorar la claridad, la previsibilidad y la confianza de los jugadores a lo largo de todo el ciclo de vida del juego.

A. IDENTIFICACIÓN DE ROLES Y RESPONSABILIDADES EN RELACIÓN CON EL RGPD

Los diferentes actores que participan en el ecosistema de los videojuegos deben determinar su rol conforme al RGPD (responsable del tratamiento, corresponsable del tratamiento o encargado del tratamiento) para comprender sus obligaciones y responsabilidades jurídicas en relación con las actividades de tratamiento de datos personales[9]. Una misma entidad puede desempeñar diferentes roles en diferentes actividades de tratamiento.

Una vez establecida como responsable del tratamiento, una entidad asume la responsabilidad principal conforme al RGPD de garantizar un tratamiento lícito, leal y transparente, incluida la implementación de medidas técnicas y organizativas adecuadas, la cooperación con las autoridades de protección de datos y la responsabilidad por todo el tratamiento posterior, incluido el realizado por encargados del tratamiento como proveedores de servicios en la nube o de tecnología publicitaria. Entre las principales obligaciones se encuentran, entre otras, identificar la base jurídica para cada actividad de tratamiento, proporcionar a los jugadores información relacionada con su privacidad clara y accesible, respetar los derechos de los interesados y mantener registros de las actividades de tratamiento y de las brechas de datos. Los responsables del tratamiento en el ecosistema de los videojuegos también deben realizar evaluaciones de impacto relativas a la protección de datos cuando el tratamiento conlleve un alto riesgo (por ejemplo, elaboración de perfiles, publicidad comportamental o tratamiento de datos de menores), establecer contratos vinculantes con los encargados del tratamiento y demostrar la protección de datos desde el diseño y por defecto a lo largo de todo el ciclo de vida del juego, desde la creación de cuentas hasta la posproducción y las operaciones en vivo.

Como ya se ha aclarado, una misma entidad puede desempeñar diferentes roles en función de la actividad específica de tratamiento. Independientemente de su rol en el sector, debe responder a estas tres preguntas fundamentales para cada actividad específica de tratamiento (creación y gestión de cuentas, telemetría, inferencia conductual) realizada a lo largo del ciclo de vida del juego:

[9] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

1. ¿Quién decidió realizar la actividad de tratamiento?
2. ¿Quién definió la finalidad (el porqué) y los medios esenciales (el cómo, como las categorías de datos y los plazos de conservación) del tratamiento?
3. ¿Quién está tratando los datos sobre la base de las instrucciones documentadas de otra entidad?

Para todos los actores, una buena práctica consiste en exigir que cada nuevo juego o funcionalidad pase por un control de roles del RGPD al final de las fases de preproducción y producción:

- **Paso 1:** Enumere las actividades de tratamiento de datos personales, al menos bajo estos tres epígrafes: creación y gestión de cuentas, telemetría e inferencia conductual. Tenga en cuenta que, durante esta etapa del ciclo de vida del videojuego, se tratarán datos personales de miembros de equipos internos (desarrollo, control de calidad, laboratorio e investigación). Asimismo, de los miembros de un círculo cercano: probadores externos (participantes en pruebas de juego seleccionados, miembros invitados de la comunidad), usuarios registrados y jugadores de acceso anticipado, etc. En esta sección, nos referiremos a todos ellos como "jugadores de acceso anticipado", y es posible que tengan o no contratos laborales con alguno de los actores del ecosistema. En etapas posteriores del ciclo de vida, se tratarán principalmente los datos personales de los "jugadores".
- **Paso 2:** Para cada actividad de tratamiento de datos personales, responda a las preguntas de orientación que se proporcionan a continuación e identifique su rol como responsable del tratamiento, corresponsable del tratamiento o encargado del tratamiento.
- **Paso 3:** Asegúrese de que se firmen acuerdos de corresponsabilidad del tratamiento (Artículo 26 del RGPD) o contratos de encargo de tratamiento de datos (Artículo 28 del RGPD) siempre que existan estas relaciones. Garantice que las políticas de privacidad, los procedimientos, las evaluaciones de impacto, etc., sean coherentes con los roles identificados. Todas estas medidas deben implementarse antes del lanzamiento del juego.

Documente sus resultados; debe poder explicar por qué eligió un rol específico del RGPD en cada caso. Además, reevalúe regularmente a medida que evolucionan los videojuegos y sus ecosistemas (por ejemplo, con la incorporación de identidades multiplataforma, la personalización basada en IA o los cambios en la telemetría).

En esta etapa específica del ciclo de vida del videojuego, puede seguir las siguientes recomendaciones por rol, siempre caso por caso, de manera específica para cada actividad de tratamiento.

IV.A.1 Proveedores de hardware

Preguntas de orientación:

- ¿Define las finalidades de la cuenta de la plataforma de hardware (control de acceso, volcados en la nube, identidad multiplataforma, soluciones antitrampa, marketing)? Si es así, usted es el responsable del tratamiento de los datos asociados a esa cuenta.
- ¿Algún desarrollador o editor codetermina qué datos deben incluirse en la cuenta de los jugadores de acceso anticipado y cómo se utilizan, por ejemplo, para pruebas o

comentarios? Si es así, considere la posibilidad de que sean corresponsables del tratamiento.

- ¿Se limita a proporcionar un SDK de inicio de sesión (sin acceso a los identificadores subyacentes, sin reutilización para sus propios fines), bajo instrucciones por escrito? Si es así, usted es el encargado de ese tratamiento.
- ¿Define qué datos de telemetría de la plataforma se recogen (duración de la sesión, uso del dispositivo, registros de errores) o qué inferencias se realizan, y los reutiliza para sus propios análisis y decisiones de producto? Si es así, es responsable del tratamiento.
- ¿Expone API de telemetría a los editores para que ambos decidan las métricas utilizadas para probar el juego? Si es así, es posible que sean corresponsables del tratamiento, especialmente cuando diseñan conjuntamente paneles de control e indicadores clave de rendimiento (*Key Performance Indicator* o KPI).

En resumen, por tipo de actividad de tratamiento de datos personales:

- Creación y gestión de cuentas (cuenta de la plataforma de hardware): probablemente responsable del tratamiento, a veces corresponsable del tratamiento o encargado del tratamiento.
- Monitorización del juego (telemetría de plataforma): responsable del tratamiento, corresponsable del tratamiento cuando la telemetría se utiliza junto con los editores.
- Inferencia conductual (inferencias de plataforma): probablemente responsable del tratamiento.

IV.A.2 Creadores, diseñadores y desarrolladores

Preguntas de orientación:

- ¿Crea cuentas de juego para probadores o personal bajo sus propios términos y política de privacidad? Si es así, usted es el responsable del tratamiento de datos asociado a esas cuentas.
- ¿Decide conservar las credenciales o los identificadores de las cuentas después del contrato para reutilizarlos en otros títulos? Si es así, tiene un rol de responsable del tratamiento independiente para esa reutilización.
- ¿Crea o gestiona cuentas de jugadores de acceso anticipado completamente bajo las instrucciones documentadas y las normas de la plataforma de un editor? Si es así, es el encargado de ese tratamiento.
- ¿Quién decide qué eventos de telemetría se instrumentan (por ejemplo, finalización de niveles, pulsaciones de botones, eventos de chat) y por qué? Si usted decide o codetermina más allá de la necesidad técnica, puede ser responsable del tratamiento o corresponsable del tratamiento.
- ¿Almacenará la telemetría en su propio entorno y la reutilizará en varios títulos para mejorar el diseño, el equilibrio de dificultad o los modelos de IA? Si es así, tiene un rol de responsable del tratamiento.
- ¿Está contractualmente obligado a recoger y reenviar la telemetría en bruto exactamente como lo especifica el editor, sin reutilización independiente? Si es así, es el encargado del tratamiento.

- ¿Entrena modelos con datos de prueba o en directo para comprender los estilos de juego e informar sobre futuros títulos más allá del proyecto que le han encargado? Si es así, es el responsable del tratamiento de ese perfilado.
- ¿Se limita a implementar modelos especificados por el editor, desplegados en su infraestructura, sin reutilizar los datos ni los resultados? Si es así, es el encargado del tratamiento.

En resumen, por tipo de actividad de tratamiento de datos personales:

- Creación y gestión de cuentas (cuentas del juego): responsable del tratamiento para sus propias cuentas de prueba; encargado del tratamiento si las cuentas se gestionan para un editor.
- Monitorización del juego (telemetría del juego): encargado del tratamiento al recoger telemetría exclusivamente para el editor; responsable del tratamiento al utilizar los datos para su propia I+D en diferentes proyectos.
- Inferencia conductual (inferencias del juego): responsable del tratamiento al crear modelos para sus propios fines; encargado del tratamiento al crear modelos exclusivamente para el editor bajo instrucciones.

IV.A.3 Proveedores de tecnología para el desarrollo

Preguntas de orientación:

- ¿Utiliza los datos de su propia cuenta de servicio (correo electrónico, nombre de usuario, uso) para gestionar licencias, ofrecer soporte y mejorar sus herramientas? Si es así, es el responsable del tratamiento de ese tratamiento.
- ¿Ofrece un inicio de sesión de marca blanca en el que todas las decisiones sobre la cuenta (campos, conservación, reutilización) las establece el cliente y usted no puede reutilizar los datos? Si es así, es el encargado del tratamiento.
- ¿Envía su servicio datos de jugadores/dispositivos a sus propios servidores por defecto (por ejemplo, información sobre fallos, contadores de rendimiento) para mejorar su producto? Si es así, es el responsable del tratamiento de esa telemetría.
- ¿Pueden los creadores, diseñadores y desarrolladores desactivar o configurar detalladamente la captura de datos, o está integrada? En los casos en los que haya menos capacidad de configuración y exista la posibilidad de que usted reutilice los datos, es más claramente el responsable del tratamiento.
- ¿Trata la telemetría únicamente en el entorno del cliente, sin acceso ni reutilización? Si es así, puede identificarse como encargado del tratamiento, pero considere que el mero código de biblioteca local sin acceso puede evitarle la decisión responsable/encargado del tratamiento del RGPD para ese tratamiento de datos específico.
- ¿Ofrece módulos genéricos de optimización de la participación o de ofertas personalizadas que todos los juegos pueden integrar, y los ajusta utilizando datos de varios juegos? Si es así, usted es el responsable del tratamiento de ese motor de perfilado, incluso si los estudios también son responsables del tratamiento por su uso.
- ¿Define conjuntamente con los estudios la lógica de segmentación para campañas específicas? Si es así, considere la corresponsabilidad del tratamiento.

- ¿Aloja y ejecuta modelos sin reutilización o decisiones independientes, y los estudios definen completamente la lógica? Si es así, puede ser el encargado del tratamiento.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas propias de servicio): responsable del tratamiento; encargado del tratamiento si se limita a autenticar para un cliente.
- Monitorización del juego (telemetría del servicio): a menudo responsable del tratamiento, a veces corresponsable del tratamiento; puede ser encargado del tratamiento si está realmente sujeto a instrucciones de otro.
- Inferencia conductual (inferencias del servicio): responsable del tratamiento para modelos conductuales genéricos (posible corresponsable del tratamiento), a veces encargado del tratamiento.

IV.A.4 Editores

Preguntas de orientación:

- ¿Decide crear identificadores del editor que vinculen al jugador en diferentes juegos, plataformas y telemetría? Si es así, es el responsable del tratamiento de ese grafo de identidad.
- ¿Una plataforma (proveedor de hardware/consola o *storefront*) codetermina cómo se vinculan sus cuentas con las suyas y para qué funcionalidades conjuntas? Si es así, son corresponsables del tratamiento.
- ¿Gestiona cuentas únicamente como servicio para otra marca bajo su logotipo y políticas? Si es así, es el encargado del tratamiento para ese tratamiento.
- ¿Diseña la estrategia de telemetría para esta etapa del ciclo de vida del videojuego (qué medir, durante cuánto tiempo y para tomar qué decisiones)? Si es así, es el responsable del tratamiento.
- ¿Combina telemetría de varias plataformas de hardware o *storefronts* para crear perfiles unificados de jugadores de acceso anticipado? Si es así, tiene el rol de responsable del tratamiento.
- ¿Los contratos con estudios o proveedores de tecnología para el desarrollo reflejan con exactitud su rol? Si usted proporciona instrucciones detalladas y prohíbe la reutilización, deberían ser encargados del tratamiento para su telemetría.
- ¿Utiliza inferencias conductuales para probar o mejorar el juego en esta etapa? Si es así, es el responsable del tratamiento del perfilado.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas del editor): responsable del tratamiento, a veces corresponsable del tratamiento con creadores, diseñadores y desarrolladores.
- Monitorización del juego (telemetría del editor): responsable del tratamiento de la telemetría; corresponsable del tratamiento con otros actores cuando codeciden.
- Inferencia conductual (inferencias del editor): responsable del tratamiento del perfilado basado en el juego; a veces corresponsable del tratamiento con proveedores de hardware, proveedores de tecnología para el desarrollo o *storefronts*.

Nota: Hay que hacer una mención especial a los "mods". Los mods son modificaciones realizadas por los usuarios en los recursos, el código, las reglas, los elementos visuales o las funcionalidades de un videojuego. Un desarrollador hace que un juego sea más modificable al proporcionar herramientas, formatos de archivo abiertos o soporte para *scripts*. Los juegos con un buen soporte para mods suelen mantener activas a las comunidades, ya que los mods aumentan el valor de rejugabilidad y la creatividad, e incluso pueden redefinir la identidad del juego. Los mods pueden reemplazar texturas, cambiar modelos de personajes, añadir objetos, ajustar el equilibrio de dificultad o modificar el grado de dicha dificultad. Los mods más avanzados inyectan *scripts* o se conectan a la lógica del juego para añadir mecánicas, interfaces de usuario o crear conversiones totales que se perciben como juegos nuevos construidos sobre el motor original.

Hay que tener en cuenta que los mods pueden redefinir los flujos de datos dentro de un juego: pueden cambiar quién recoge los datos, qué datos se recogen y quién es responsable de ellos conforme al RGPD. Un mod puede añadir funcionalidades en línea, conectarse a servidores externos, registrar el comportamiento de juego o integrar SDKs. Estos SDK pueden tratar identificadores, direcciones IP, datos del dispositivo o contenido de voz/vídeo. Esto significa que la pregunta no es solo ¿está permitido el mod?, sino también ¿quién es el responsable del tratamiento, quién es el encargado del tratamiento y qué base jurídica aplica? En la práctica, el ecosistema de mods puede generar riesgos completamente nuevos. Esto afecta a los editores de juegos, las plataformas de mods, los operadores de servidores y los creadores de mods, especialmente cuando los mods utilizan telemetría, cuentas, chat, voz, analítica, sistemas antitrampa o servicios de terceros.

Si el editor simplemente proporciona un conjunto de herramientas para *modding* pero no decide el tratamiento de datos del mod, el creador del mod o el servicio de mods pueden asumir la responsabilidad principal de su propio tratamiento. Pero si el editor promueve, preinstala, selecciona o habilita técnicamente la recolección de datos del mod, el editor aún puede tener obligaciones conforme al RGPD y puede estar sujeto a un análisis de corresponsabilidad del tratamiento.

IV.A.5 *Storefronts*

Preguntas de orientación:

- ¿Reutiliza los datos de la cuenta para el historial de compras entre juegos, las recomendaciones y las funcionalidades sociales que usted define? Si es así, es el responsable del tratamiento.
- ¿Diseña usted y un editor específico, conjuntamente, un sistema de fidelización o progresión que requiera cuentas compartidas? Si es así, son corresponsables del tratamiento de ese sistema.
- ¿Recopila telemetría a nivel del lanzador (tiempo en el lanzador, clics, búsquedas, tiempo en cada título) para mejorar su propia experiencia de usuario, recomendaciones y pruebas A/B? Si es así, es el responsable del tratamiento.
- ¿Permite que los editores integren sus propias etiquetas de telemetría, pero usted no decide los fines/medios ni reutiliza los datos? Si es así, probablemente sean responsables del tratamiento independientes, y usted proporciona la infraestructura.
- ¿Diseña en conjunto programas de analítica (por ejemplo, experimentos de promoción cruzada en los que usted y el editor seleccionan segmentos y métricas)? Si es así, evalúe si hay corresponsabilidad del tratamiento.
- ¿Perfila el comportamiento de los jugadores de acceso anticipado en la tienda y en el juego para recomendar títulos, promocionar eventos específicos o personalizar ofertas? Si es así, es el responsable del tratamiento.

- ¿Realiza campañas de marketing conjuntas en las que usted y un editor codeterminan los criterios de segmentación? Si es así, verifique si hay corresponsabilidad del tratamiento. Como mínimo, ambos son responsables del tratamiento que intercambian perfiles.

En resumen, por tipo de actividad de tratamiento de datos personales:

- Creación y gestión de cuentas (cuenta del *storefront*): responsable del tratamiento; posiblemente corresponsable del tratamiento con editores para programas de marca compartida.
- Monitorización del juego (telemetría del *storefront*): responsable del tratamiento de la telemetría utilizada para gestionar y optimizar la tienda/lanzador; corresponsable del tratamiento si codecide la telemetría con los editores.
- Inferencia conductual (inferencias del *storefront*): responsable del tratamiento de sus propios sistemas de recomendación y publicidad dirigida; a veces corresponsable del tratamiento con editores para campañas conjuntas.

B. IDENTIFICACIÓN DE ACTIVIDADES DE TRATAMIENTO, FINALIDADES Y BASES JURÍDICAS

IV.B.1 Creación del registro de actividades de tratamiento

Antes de lanzar el videojuego, los responsables del tratamiento deben elaborar un inventario o registro exhaustivo que describa todas las categorías de datos personales que tratarán en todas las etapas del ciclo de vida del videojuego, no solo en esta primera. Esto incluye identificadores evidentes, como nombres de usuario, direcciones de correo electrónico y direcciones IP, así como otras categorías no tan evidentes pero comunes en los videojuegos, como la telemetría y la inferencia de comportamiento. Además, una descripción de las categorías de interesados, las categorías de destinatarios (y, cuando sea aplicable, las transferencias de datos personales a un tercer país o a una organización internacional) y los plazos de conservación.

Es esencial identificar por separado las categorías especiales de datos personales, es decir, los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, o datos genéticos, datos biométricos dirigidos a identificar de manera unívoca, datos relativos a la salud o datos relativos a la vida u orientación sexual (Artículo 9 RGPD). Todos los actores deben prohibir explícitamente la recogida de categorías especiales por defecto, por ejemplo, mediante reglas de interfaz para prohibir campos abiertos de “biografía” y el diseño de filtros para anonimizar el contenido de los chats o las etiquetas de comportamiento que puedan revelar información sensible.

Durante las fases de preproducción y producción de un videojuego, que abarcan desde la presentación inicial hasta los preparativos finales previos al lanzamiento, todos los actores del ecosistema deben adoptar un enfoque proactivo hacia la protección de datos para cumplir con los requisitos del Artículo 5 del RGPD. Cada categoría de datos debe estar claramente vinculada a un fin determinado, explícito y legítimo. Las formulaciones genéricas, como “mejorar el juego” o “mejorar la experiencia del jugador”, no cumplen con el Artículo 5(1)(b). En su lugar, las descripciones de los fines deben reflejar los casos de uso reales de la manera más transparente y detallada posible, como “detectar errores”, “equilibrar la dificultad”, “perfeccionar el emparejamiento” o “detectar trampas”.

Para mantener los principios de licitud, lealtad y transparencia, todos los actores deben comenzar definiendo esquemas de datos estrictos para la creación de cuentas y eliminando los campos “que sería bueno tener” pero que no apoyen directamente los fines definidos. Esto significa especificar atributos exactos para las cuentas de desarrollador, SDK, probador o jugador, y prohibir etiquetas arbitrarias o campos de texto libre que puedan incorporar involuntariamente datos personales de los interesados.

La limitación de la finalidad y la minimización de datos se cumplen en mayor medida cuando los actores justifican cada evento de telemetría o inferencia en relación con fines específicos, como “necesidad técnica” o “analítica” en sus especificaciones de diseño. Los responsables deben seguir la evolución del hardware, los sistemas operativos y la tecnología de desarrollo y sus funcionalidades, en particular en lo que respecta a la minimización de los datos tratados (por ejemplo, la recogida de identificadores, direcciones de red o geolocalización).

Es crucial que la limitación del almacenamiento se codifique desde el principio; los actores deben documentar los plazos de conservación (por ejemplo, eliminar cuentas de prueba de juego o registros de telemetría en bruto entre 30 y 90 días después de una fase de prueba) e implementar estas reglas mediante purgados automatizados o *scripts* en la planificación de lanzamiento.

La responsabilidad proactiva se refuerza cuando estas decisiones se registran en listas de comprobación del proyecto o diccionarios de datos. Toda esta información también es esencial para redactar políticas de privacidad precisas, diseñar flujos de consentimiento e identificar actividades de tratamiento de alto riesgo que requieran una evaluación de impacto relativa a la protección de datos (EIPD) conforme al Artículo 35.

IV.B.2. Documentación de la base jurídica para cada finalidad

Tras determinar los fines de cada actividad de tratamiento, cada una debe asociarse a una base jurídica conforme al Artículo 6. La naturaleza específica de las actividades de tratamiento y la variedad de fines perseguidos suelen requerir el uso de diferentes bases jurídicas para distintas actividades de tratamiento:

- Consentimiento (Artículo 6(1)(a)), por ejemplo, para la personalización opcional, la publicidad comportamental, la elaboración de perfiles entre plataformas y cualquier tratamiento que vaya más allá de las expectativas razonables del jugador de un videojuego.
- El tratamiento es necesario para la ejecución de un contrato (Artículo 6(1)(b)), por ejemplo, para funciones esenciales del juego y la creación de cuentas.
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (Artículo 6(1)(f)), por ejemplo, para análisis de seguridad o estabilidad proporcionados, sujetos a una prueba de ponderación rigurosa[10].
- El tratamiento es necesario para el cumplimiento de una obligación legal (Artículo 6(1)(c)), por ejemplo, para requisitos contables y normativos asociados a las compras.

En principio, no existe jerarquía a la hora de determinar en qué base jurídica basarse para una actividad de tratamiento concreta. Es responsabilidad del responsable del tratamiento justificar la base jurídica adecuada para cada actividad de tratamiento.

[10] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

Una tarea fundamental en estas primeras etapas de un videojuego es distinguir entre las funcionalidades que requieren el tratamiento de datos personales, y que son estrictamente necesarias para ejecutar el juego, y aquellas que son opcionales, complementarias o impulsadas por la monetización. Después de todo, el RGPD exige a los responsables del tratamiento que basen cada actividad de tratamiento en una de las seis bases jurídicas enumeradas en el Artículo 6 del RGPD, y los criterios de necesidad pueden influir en la elección de una base jurídica u otra. También exige a los responsables del tratamiento que identifiquen el fin de cada actividad de tratamiento antes de que esta comience. Una vez establecidas la base jurídica y el fin de una actividad de tratamiento concreta, los datos personales recogidos durante dicha actividad no pueden, en principio, utilizarse ulteriormente de manera incompatible con el fin original. Para ello, sería necesaria una base jurídica independiente.

Muchos actores pueden enfrentarse a dificultades más adelante en el ciclo de vida cuando se den cuenta de que los datos personales recogidos inicialmente para "mejorar el juego" se están reutilizando para publicidad dirigida o monetización basada en la participación. Si estas distinciones no se reconocen formalmente durante la preproducción, el desvío o desvirtuación de finalidad (*function creep*) se vuelve casi inevitable, lo que plantea graves problemas en virtud del principio de limitación de la finalidad.

Por lo tanto, documentar adecuadamente los fines y las bases jurídicas de cada actividad de tratamiento es esencial para el cumplimiento y debe hacerse lo antes posible en esta etapa del ciclo de vida del juego.

IV.B.3 Soporte a la responsabilidad proactiva, la gobernanza y la gestión del ciclo de vida

El principio de responsabilidad proactiva exige a los responsables del tratamiento demostrar no solo el cumplimiento, sino un cumplimiento estructurado y documentado. Un mapa detallado del ciclo de vida de los datos que muestre cómo cada categoría de datos entra en el ecosistema, se procesa, almacena, transfiere, conserva y suprime, sirve como un artefacto central de cumplimiento. Esta documentación también apoya el cumplimiento de otros requisitos establecidos en el RGPD, como:

- Evaluaciones de transferencias internacionales conforme al Capítulo V[11].
- Gobernanza interna conforme al Artículo 24.
- Acuerdos de corresponsabilidad conforme al Artículo 26.
- Acuerdos y contratos con encargados del tratamiento conforme a los Artículos 28 y 29.
- Evaluaciones de impacto relativas a la protección de datos conforme al Artículo 35.

Un mapa detallado del ciclo de vida ayuda a los equipos de desarrollo y operaciones en vivo a mantener un modelo mental compartido de los datos de los que son responsables de crear, transformar o proteger.

En cuanto a las transferencias internacionales conforme al Capítulo V, es esencial que los responsables del tratamiento identifiquen, lo antes posible en el ciclo de vida del juego, la ubicación de los servidores, las decisiones de adecuación, las cláusulas contractuales tipo y las evaluaciones de riesgo de las transferencias, para evitar decisiones de diseño y arquitectura que no cumplan con la norma y que sean difíciles de corregir más adelante.

Es fundamental conocer el efecto "muñecas rusas" en los videojuegos: la cadena anidada de SDK en la que la integración de una tecnología de desarrollo principal incorpora

[11] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en

automáticamente múltiples sub-SDK de terceros, creando capas opacas de encargados del tratamiento que los responsables a menudo no mapean o controlan fácilmente. Estos deben exigir a sus encargados declaraciones completas de subencargados y rechazar la mediación de "caja negra". Deben requerir notificación/autorización previa del responsable para los cambios en los subencargados (Artículo 28(2) del RGPD) y establecer límites, por ejemplo, "sin muñecas más allá de 2 niveles". Se recomienda utilizar escáneres de SDK y herramientas similares en los procesos de CI/CD[12] para identificar estos anidamientos en esta etapa del ciclo de vida. Además, recurrir a integraciones directas o soluciones locales por defecto (por ejemplo, sin recurrir a publicidad en la nube) para las configuraciones predeterminadas. Los proveedores de tecnología para el desarrollo deben diseñar sus servicios de modo que las funcionalidades como el análisis de audiencias o el *retargeting* publicitario estén desacopladas, permitiendo a los clientes seleccionar solo los módulos de software que necesitan para minimizar estas integraciones.

Los proveedores de hardware deben indicar claramente en los kits de desarrollo y la documentación qué flujos de telemetría están bajo su control y cuáles se proporcionan como "tuberías" (flujos de datos) para los editores. Para los paneles de control conjuntos, deben incluir una sección breve de corresponsabilidad en los contratos con los socios que cubra las bases jurídicas, las obligaciones de transparencia, las responsabilidades en caso de brecha de datos y el ejercicio de los derechos de los interesados. Además, deben clasificar cada inferencia de comportamiento (por ejemplo, "predicción de abandono") por su impacto potencial, como la optimización de la experiencia de usuario, la segmentación para monetización o la seguridad, elaborando secciones específicas de EIPD tan pronto como se identifiquen escenarios de alto riesgo. En esta etapa, también es crucial la etiqueta "menores implicados" (véase la sección IV.D.1 más adelante).

Si es creador, diseñador o desarrollador, para cada almacenamiento de cuentas (herramientas de control de calidad, seguimiento de errores, portales alfa/beta), debe registrar el fin, quién decide el contenido y la conservación, y si se reutilizará. Cuando actúe como encargado del tratamiento, rechace las instrucciones verbales: exija instrucciones por escrito, incluidas las relativas a la conservación y supresión al final del proyecto. En cada plan de analítica, etiquete cada evento con: "solo para el editor" vs "reutilización por el estudio". Esta última opción requiere su propia base jurídica y registros del tratamiento. Para las pruebas externas de juego, prepare una plantilla de aviso de telemetría que explique qué se registra durante las pruebas, quién puede acceder a esos datos y durante cuánto tiempo se conservan. Esta información debe alinearse con las políticas del editor. Finalmente, al definir funcionalidades de IA/personalización en preproducción, añada una hoja de roles de elaboración de perfiles por modelo: quién es el propietario, quién puede reutilizarlo y si actúa como responsable o como encargado del tratamiento. Para mecánicas de alto impacto más adelante en el ciclo de vida del juego (por ejemplo, precios dinámicos o maximización de la participación de menores), sugiera al editor que realice una EIPD conjunta.

Los proveedores de tecnología para el desarrollo deben separar las cuentas de "usuario de la herramienta" (para equipos de desarrollo) de las cuentas de "jugador" creadas a través de su servicio. Deben proporcionar textos modelo para que los estudios expliquen claramente si comparten el control de la autenticación (por ejemplo: "X autentica tu cuenta en nuestro nombre"). Estos proveedores deben ofrecer un diagrama de flujo de datos por producto que enumere explícitamente los elementos de datos, los destinatarios, el rol de responsable o encargado y las opciones de configuración. Además, deben incluir cláusulas contractuales estándar, como: "Tú (estudio) eres el responsable del tratamiento para X; nosotros (proveedor) somos responsables para la telemetría Y; para Z, somos tu encargado del tratamiento bajo estas instrucciones". Se recomienda encarecidamente que publiquen

[12] CI/CD (Continuous Integration and Continuous Deployment/Delivery) es una metodología DevOps que automatiza la creación, las pruebas y la publicación de software.

una hoja de datos de elaboración de perfiles detallada para cada módulo de comportamiento, que incluya las entradas, salidas, fines, el responsable del tratamiento y cómo pueden ejercer sus derechos los interesados.

Durante la preproducción, los editores deben decidir si el juego utilizará cuentas exclusivas de la plataforma, cuentas del editor o un sistema híbrido, y realizar una lista de comprobación de roles para cada opción. Para los registros en versiones alfa/beta, deben mantener una entrada separada en el registro que documente qué datos recogen (correos electrónicos, edad, IDs de plataforma) y si los utilizarán más adelante para marketing o futuros títulos (en cuyo caso, serán los responsables del tratamiento para este tratamiento). En los acuerdos alfa/beta con los probadores, los editores deben especificar si la telemetría está anonimizada/agregada y si se utilizará para futuros títulos o elaboración de perfiles, ajustando los mecanismos de transparencia y elección o toma de decisiones en consecuencia.

Para los *storefronts*, al configurar programas alfa/beta a través de la tienda, deben aclarar en los contratos qué consentimientos/avisos muestra la tienda, qué datos recibe el editor y bajo qué rol (responsable independiente o encargado del tratamiento). Deben proporcionar a los editores un documento resumen de roles para cada programa, para que ambas partes puedan alinear sus políticas de privacidad o las EIPD. También deben facilitar a los editores una guía clara de roles de telemetría que distinga entre el análisis de la tienda (bajo su responsabilidad como responsables) y el análisis por juego (bajo la responsabilidad del editor/estudio). Por último, para cada modelo de recomendación/segmentación, deben documentar qué fuentes de datos se utilizan (por ejemplo, solo comportamiento en la tienda o también telemetría en el juego).

C. CONCEPTUALIZACIÓN Y DISEÑO DE LAS MECÁNICAS DEL JUEGO

IV.C.1 Inclusión de la protección de datos desde el diseño y por defecto

El Artículo 25 del RGPD exige a los responsables del tratamiento integrar garantías de protección de datos tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento[13]. En el contexto de los videojuegos, esta obligación es profundamente relevante para la conceptualización y el diseño de un videojuego. Para cuando los juegos comienzan a refinarse, muchas decisiones sobre flujos de datos, elaboración de perfiles de jugadores y arquitectura *backend* ya se han tomado. Por lo tanto, la protección de datos desde el diseño debe estar presente en la mente de quienes manejan el diseño operativo, así como el creativo del juego.

Para creadores, diseñadores y desarrolladores, este principio es, por tanto, una consideración creativa que define qué mecánicas son permisibles sin un tratamiento desproporcionado de los datos personales de los jugadores. Un diseñador de juegos que tenga que decidir si el progreso debe estar vinculado a identificadores persistentes, por ejemplo, está tomando una decisión de privacidad tanto como una decisión narrativa o de sistemas. Si la validación de logros o la evaluación de habilidades puede realizarse localmente (por ejemplo, a través de datos almacenados en el dispositivo) en lugar de mediante cargas continuas de telemetría a un servidor externo, el diseño debe favorecer siempre la opción menos intrusiva.

[13] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

En la práctica, tratar la privacidad como un parámetro de diseño central suele llevar a la adopción de enfoques alternativos y respetuosos con la privacidad, como niveles de emparejamiento basados en agregados o por sesión en lugar de en perfiles de comportamiento detallados, o la separación técnica de los registros necesarios para seguridad/antifraude (necesidad estricta) de otros registros utilizados para UX (*User eXperience*) o marketing, por ejemplo.

El procesamiento local en videojuegos encarna perfectamente la protección de datos desde el diseño y por defecto del Artículo 25 del RGPD al minimizar la transmisión de datos a servidores externos, reducir la exposición a brechas y limitar la elaboración de perfiles centralizada en todo el ecosistema. Buenos ejemplos son los sistemas de progreso local para géneros fuera de línea o de un solo jugador, reduciendo la dependencia de cargas persistentes a un servidor externo a través de cuentas o el cómputo en el dispositivo para funcionalidades de realidad virtual o seguimiento de movimiento, minimizando la transmisión de firmas de comportamiento potencialmente sensibles.

Este enfoque incorpora la protección por defecto, sin transmisión al servidor: los datos personales como la telemetría o incluso inferencias de comportamiento básicas permanecen en el dispositivo, eliminando muchos riesgos durante la recogida y el uso inicial. Solo los resultados agregados o estrictamente necesarios llegan a los servidores, evitando cargas masivas de datos personales en bruto. El tratamiento se realiza en hardware propiedad del usuario y bajo su control, dando a los jugadores la posibilidad de una supervisión inherente. Esta debería ser la manera de trabajar por defecto para funcionalidades sensibles; las nuevas actualizaciones o juegos deben lanzarse con una lógica local por defecto, haciendo que “local” sea la opción predeterminada a menos que el jugador opte de manera explícita por la sincronización en la nube.

De igual forma, los campos de cuenta opcionales, las funcionalidades de grafo social y el uso compartido de datos con terceros deben estar configurados como “desactivados” por defecto, requiriendo una acción explícita para su activación. En la práctica, esto significa que la analítica opcional no debe activarse silenciosamente después de la creación de la cuenta, la configuración de descubrimiento multijugador debe ser privada o solo para amigos por defecto cuando sea factible, y funcionalidades que incluyan la personalización basada en el comportamiento deben requerir una activación mediante un consentimiento explícito, por ejemplo. Además, una buena práctica es restablecer el regreso de jugadores inactivos a la configuración de privacidad máxima (sin elaboración de perfiles entre títulos, sin amigos compartidos): un jugador regresa a una plataforma después de un año; en lugar de ser mostrado instantáneamente a todos los amigos, añadido automáticamente a listas de “recientemente de vuelta” entre juegos y activado el perfilado en todos los títulos que posee, vuelve a juegar en un modo silencioso por defecto donde su presencia es mayoritariamente privada a menos que y hasta que active explícitamente más funcionalidades sociales y personalizadas. Los proveedores de tecnología para el desarrollo deben asegurarse de que sus paneles de control de SDK muestren solo métricas agregadas. El acceso a la telemetría de jugador en bruto debe requerir un proceso de escalada de privilegios con límite de tiempo y registrado, no accesible para todos.

Durante la instrumentación, los editores deben etiquetar los eventos individuales de telemetría como “esenciales” frente a “no esenciales” para garantizar que los controles de privacidad puedan desactivar estos últimos para los jugadores. Los proveedores de hardware y de tecnología para el desarrollo deben ofrecer indicadores de configuración que permitan a los clientes desactivar por completo las funciones de elaboración de perfiles, por ejemplo, en regiones geográficas específicas. Las herramientas de elaboración de perfiles deben modularizarse, asegurando que los datos de elaboración de perfiles recogidos con fines de seguridad o emparejamiento basado en habilidades estén estrictamente separados de los datos de elaboración de perfiles recogidos con fines de monetización para evitar la

explotación de vulnerabilidades de los jugadores. En general, los proveedores de tecnología para el desarrollo deben ofrecer indicadores de configuración que permitan a los estudios desactivar usos de alto riesgo (por ejemplo, relativos a menores) y documentar estos como parte de las medidas de protección de datos por defecto. Además, los *storefronts* deben diseñar sus sistemas de modo que el uso compartido de identificadores con editores utilice *tokens* de alcance limitado en lugar de registros de cuenta completos.

IV.C.2 Integración de la privacidad en la narrativa y el diseño social

Los creadores, diseñadores y desarrolladores integran cada vez más PNJ impulsados por inteligencia artificial para mejorar la inmersión, la narrativa dinámica y la personalización. Estos PNJ suelen tratar datos de los jugadores, como mensajes de chat, comandos de voz, elecciones de juego y patrones de comportamiento, para generar respuestas, adaptar narrativas o aplicar moderación de contenidos.

Cada funcionalidad de un PNJ que recoja o infiera datos de los jugadores debe tener asociada una base jurídica válida. La lealtad exige evitar resultados discriminatorios de los modelos de IA, por lo que las auditorías regulares para detectar sesgos en la toma de decisiones de los PNJ, como la personalización de diálogos o la asignación de recompensas, ayudan a garantizar un trato equitativo entre los diferentes grupos demográficos de jugadores. Los responsables del tratamiento deben revelar las prácticas de datos de los PNJ a través de avisos contextuales (por ejemplo, descripciones emergentes que expliquen: “Esta IA recuerda tus elecciones para personalizar las misiones”) y políticas de privacidad completas que detallen los flujos, la conservación y la participación de la IA.

El tratamiento de datos de los PNJ debe limitarse estrictamente a los fines de juego predefinidos, como la adaptación en tiempo real o la detección de trampas, con salvaguardas en el código que eviten la derivación hacia el marketing o la analítica externa sin una base jurídica adecuada. Los responsables del tratamiento deben complementar este enfoque con la minimización de datos, capturando solo los elementos esenciales. Por ejemplo, resumir las intenciones del chat en lugar de almacenar transcripciones completas, y aplicar la purga automática de las entradas en bruto tras el tratamiento.

Los PNJ impulsados por IA deben priorizar la precisión, validando los perfiles inferidos de los jugadores mediante bucles de retroalimentación, permitiendo correcciones a través de interfaces sencillas en el juego para rectificar errores en las preferencias o comportamientos recordados. Los responsables del tratamiento deben combinar estas medidas con la limitación de conservación mediante políticas de conservación por niveles: efímero para datos vinculados a la sesión, a corto plazo para la continuidad entre sesiones y de forma indefinida solo para agregados anonimizados. Para permitir a los interesados tomar el control de sus datos, las interacciones con PNJ y los menús de los jugadores deben integrar herramientas de derechos fluidas, como reinicios de memoria con un clic, exportaciones de datos o formularios para ejercer el derecho de oposición.

Por último, el entrenamiento de PNJ impulsados por IA en juegos implica alimentar los modelos con datos de interacción de los jugadores (registros de chat, elecciones, patrones de voz, etc.) para permitir comportamientos adaptativos. En este caso, se aplicarían las mismas recomendaciones que para el entrenamiento de otros modelos de IA que no se utilicen en videojuegos. Una de las esenciales es recurrir a datos sintéticos cuando sea posible y, en el resto de los casos, minimizar el conjunto de datos de entrenamiento mediante la agregación o pseudonimización de las entradas, sustituyendo los identificadores por *tokens* y eliminando detalles innecesarios, como marcas de tiempo o ubicaciones, antes de usarlos para entrenar los modelos, asegurando que solo se conserven los patrones indispensables (por ejemplo, estilos de diálogo). Se recomiendan encarecidamente

auditorías previas al entrenamiento para verificar que no persistan identificadores directos o indirectos.

Los juegos modernos incorporan cada vez más espacios sociales como salones de emparejamiento, cuarteles generales, vestíbulos o salas de espera, canales de chat de voz o texto, entornos de comercio y centros de contenido generado por los usuarios. Estos sistemas permiten la creatividad de los jugadores y la creación de comunidades, pero también introducen amenazas considerables para la privacidad. Por lo tanto, la inclusión de funcionalidades sociales debe abordarse con una comprensión clara de las implicaciones para la limitación de la finalidad, la elaboración de perfiles y la lealtad, especialmente cuando hay menores presentes.

Los diferentes actores deben hacerse preguntas como:

- ¿Son las funcionalidades sociales realmente opcionales o se impedirá a los jugadores acceder al contenido principal si no interactúan con ellas o a través de ellas?
- ¿Las comunicaciones serán moderadas por medios automatizados, almacenadas de forma persistente o analizadas para la elaboración de perfiles de comportamiento?
- ¿Los sistemas de reputación o confianza se basan en datos de comportamiento extensos que podrían influir indebidamente en la experiencia o autonomía de los jugadores?
- ¿Las invitaciones no solicitadas, las solicitudes de amistad o las interacciones públicas podrían exponer a los NNA a contenido inapropiado o a comportamientos manipuladores? ¿Existen paneles para padres y tutores, o herramientas equivalentes, que les permitan desactivar el chat de voz, restringir las invitaciones de amigos o revisar la configuración de las herramientas de comunicación?

Abordar estas cuestiones desde las primeras etapas del diseño del juego evita la creación de sistemas que serían técnica o económicamente imposibles de modificar más adelante. También garantiza que la protección de la integridad de los jugadores y de su seguridad no se incorpora a posteriori, sino que se integra de forma natural en el mundo del juego.

IV.C.3 Evitación del diseño engañoso y adictivo

Cada actor que participe en telemetría o inferencia de comportamiento debe asegurarse de que sus propias interfaces y acuerdos contractuales no permitan ni incluyan patrones de diseño engañosos o adictivos, y de que las opciones que cumplen con el RGPD se propaguen a través de toda la pila de juego.

Los patrones engañosos y adictivos, como flujos de consentimiento manipulativos, cajas botín programadas para generar frustración o incentivos que explotan vulnerabilidades de gasto, suelen basarse en datos de telemetría (patrones de juego, entradas, duración de las sesiones) e inferencia de comportamiento (riesgo de abandono, propensión a gastar grandes sumas). Esto infringe diversos principios y requisitos del RGPD, incluidos los Artículos 5, 9 y 25[14],[15].

Los responsables del tratamiento deben diseñar interfaces de privacidad con la misma fricción para aceptar/rechazar y que eviten casillas premarcadas, *confirmshaming* ("¿Rechazar y perder recompensas?") u opciones de exclusión disfrazadas. Deben separar claramente, por ejemplo, los consentimientos para la telemetría esencial del juego de los consentimientos para realizar perfiles de monetización y evitar el uso de inferencias para

[14] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[15] AEPD Report on addictive patterns in the processing of personal data: Implications for data protection, https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf

personalizar la presión (por ejemplo, ofertas durante rachas de derrotas), ya que esto socava la lealtad y corre el riesgo de invalidar el consentimiento en toda la cadena.

Además, los responsables del tratamiento deben recoger solo la telemetría esencial para los fines declarados, separando los datos de "seguridad/analítica" de los modelos de monetización. Deben limitar las ventanas de perfil (por ejemplo, las últimas 3 sesiones) para evitar perfiles "de por vida" y prohibir explícitamente la derivación/almacenamiento de inferencias de debilidad o vulnerabilidad (por ejemplo, señales de adicción o estrés financiero) para el ajuste de la participación, ya que estas se aproximan peligrosamente a las categorías especiales de datos conforme al Artículo 9 del RGPD.

Los editores y *los storefronts* están en una posición privilegiada para prevenir el diseño perjudicial; pueden, por ejemplo, incentivar a creadores, diseñadores y desarrolladores a no utilizar patrones de diseño adictivos que hagan que los jugadores quieran seguir conectados por la combinación de recompensas rápidas, progresión, presión social, escasez y objetivos personalizados.

Las cajas botín son otra gran preocupación. Una caja botín es un "paquete misterioso" dentro del juego, un objeto virtual consumible que oculta su contenido hasta que se abre; el jugador solo conoce los posibles tipos o rarezas de los objetos (comunes, raros, épicos, etc.), pero no el resultado exacto (recompensas de tipo cosmético, armas, paquetes de cartas, etc.). Pueden obtenerse durante el juego o comprarse directamente, y muchos sistemas utilizan señales visuales (iluminación, codificación por colores de la rareza) y mecánicas de "tiro garantizado" para animar a los jugadores a seguir abriendo más cajas botín. Las cajas botín se basan en el refuerzo intermitente de razón variable, el mismo principio en el que se basan las máquinas tragaperras: las recompensas son impredecibles, lo que activa fuertemente el sistema de recompensa del cerebro y hace que los jugadores lo sigan intentando "una vez más". Esto puede interactuar con rasgos como la impulsividad, la necesidad de novedad o la tendencia al juego. Si no se consideran y regulan plenamente como actividades de juego, los responsables de los tratamientos asociados deben prohibir estas cajas para NNA y hacerlas opcionales para el resto de los jugadores (por ejemplo, con opciones de "compra directa" junto a las cajas aleatorias). Cuando los jugadores interactúen con cajas botín, se requiere transparencia total y divulgación de información como las probabilidades de éxito y las estadísticas de gasto.

Además, los sistemas cosméticos, como *skins*, ropa y personalización de avatares son especialmente preocupantes porque pueden contribuir a esa atracción al fortalecer la identificación con el personaje y hacer que la autoexpresión resulte muy significativa. En términos sencillos, cuando un jugador se siente conectado con su personaje a nivel emocional, es decir, "este personaje es una extensión virtual de mí", cambiar su apariencia puede convertirse en una experiencia emocionalmente gratificante en lugar de puramente estética. Los cosméticos pueden volverse especialmente atractivos cuando están vinculados a la progresión, eventos de tiempo limitado, rareza, visibilidad social o señalización de estatus. Esto significa que una *skin* no es solo una elección visual; también puede señalar prestigio, pertenencia, gusto o logro, lo que puede hacer que los jugadores persigan repetidamente tener nuevos aspectos en el juego.

Comprender las motivaciones de los jugadores también es importante. Diferentes jugadores pueden sentirse atraídos por ciertas funcionalidades por diferentes razones. Algunos disfrutan de la autoexpresión y la experimentación, otros quieren coincidir con una identidad preferida, otros buscan reconocimiento de otros jugadores, y algunos están motivados por el perfeccionismo o el miedo a perderse algo cuando los cosméticos se ofrecen solo por un tiempo limitado. Los patrones comunes que amplifican la participación incluyen tiendas rotativas o artículos estacionales que crean urgencia, *skins* raras o exclusivas que generan presión de estatus, rutas de progresión que premian el juego

repetido con desbloqueos cosméticos, sistemas de visualización social, como *emotes*, vestíbulos, perfiles, insignias clasificatorias o paquetes, y microtransacciones que fomentan el gasto repetido o el comportamiento asociado a la colección.

La preocupación no es que los cosméticos o características de diseño similares sean intrínsecamente dañinos. La preocupación es que, cuando se combinan con bucles de refuerzo fuertes, presión de monetización y tácticas de escasez, estas prácticas pueden explotar a jugadores vulnerables, especialmente aquellos que son más jóvenes, muy sensibles al estatus o propensos al gasto compulsivo o al juego repetido. Por esta razón, se recomienda encarecidamente realizar pruebas de UX para detectar patrones engañosos y adictivos mediante auditorías independientes antes del lanzamiento del juego.

D. ANTICIPACIÓN DE LOS RIESGOS CON UN ÉNFASIS ESPECIAL EN LA INFANCIA

IV.D.1 Realización de una EIPD para los tratamientos de alto riesgo

Una EIPD es un proceso diseñado para describir una actividad de tratamiento de datos personales (o múltiples actividades de tratamiento similares), evaluar su necesidad y proporcionalidad, y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados de dicho tratamiento, mediante su evaluación y la determinación de las medidas para abordarlos[16]. Las EIPD son herramientas muy importantes para la responsabilidad proactiva, ya que implican un proceso para construir y demostrar el cumplimiento.

En línea con el enfoque basado en el riesgo del RGPD, la realización de una EIPD no es obligatoria para toda operación de tratamiento. Una EIPD es necesaria cuando el tratamiento "entrañe un alto riesgo para los derechos y libertades de las personas físicas". Algunos ejemplos son la evaluación sistemática o puntuación (incluyendo la elaboración de perfiles y la predicción), especialmente en aspectos relativos al rendimiento laboral del interesado, su situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos; la toma de decisiones automatizada con efectos jurídicos o similares de importancia significativa; la vigilancia sistemática; datos sensibles o de naturaleza altamente personal (esto incluye las categorías especiales de datos personales definidas en el Artículo 9 del RGPD); datos tratados a gran escala; la interconexión o combinación de conjuntos de datos; datos relativos a interesados vulnerables; el uso innovador o la aplicación de nuevas soluciones tecnológicas u organizativas, y cuando el tratamiento en sí impida a los interesados ejercer un derecho o utilizar un servicio o un contrato.

Las secciones anteriores ya han mostrado que varias funcionalidades de los juegos pueden implicar actividades de tratamiento de alto riesgo conforme a estos criterios, requiriendo por tanto una EIPD antes del lanzamiento. Entre las actividades de tratamiento que pueden requerir una EIPD se incluyen la elaboración de perfiles de comportamiento extensivos, la moderación automatizada de contenidos, la toma de decisiones en los sistemas antitrampa, el tratamiento de datos de menores, el tratamiento de datos sensibles recogidos mediante sensores y BCIs, incluidos los datos biométricos, y las funcionalidades basadas en la ubicación.

El RGPD especifica el alcance de una EIPD y el contenido que debe incluir (Artículo 35 del RGPD). Al realizar una EIPD, el responsable del tratamiento debe asegurarse de que incluya una descripción sistemática de las operaciones de tratamiento en cuestión y sus

[16] WP Article 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

fines. El responsable también debe evaluar la necesidad y proporcionalidad de la actividad de tratamiento en relación con los fines mencionados, así como los riesgos que la actividad de tratamiento puede tener sobre los derechos y libertades de los interesados afectados. Finalmente, la EIPD debe incluir las medidas previstas para abordar los riesgos identificados. Si, tras la evaluación, el responsable del tratamiento concluye que el riesgo residual sigue siendo alto, el Artículo 36 exige una consulta previa con la autoridad de control competente.

Las EIPD no deben considerarse como un mero trámite legal, sino como herramientas creativas y técnicas útiles para el diseño de juegos conforme al RGPD y de manera responsable. A menudo revelan que los objetivos de juego pueden alcanzarse con un tratamiento de datos menos intrusivo. Por ejemplo, trasladando el cómputo sensible al dispositivo, reduciendo los plazos de conservación de datos o introduciendo supervisión humana en los procesos de moderación automatizada.

Incluso si no se activa la obligación de realizar una EIPD, los responsables del tratamiento deben implementar medidas para gestionar los riesgos para los derechos y libertades de los interesados. Además, los responsables del tratamiento deben evaluar de manera continua los riesgos derivados de sus actividades de tratamiento para identificar cuándo el tratamiento puede entrañar un alto riesgo para los derechos y libertades de las personas.

IV.D.2 Reconocimiento de las vulnerabilidades específicas de la infancia en el contexto de la protección de datos

Los NNA son uno de los grupos de participantes más activos en los entornos de juego, y su presencia modifica fundamentalmente las responsabilidades del responsable del tratamiento. Conforme al Artículo 5(1)(a), el tratamiento debe ser leal, y la lealtad para estos sujetos de datos exige normas de protección reforzadas. Los NNA pueden no comprender plenamente el alcance y los riesgos de ciertas prácticas de tratamiento de datos, pueden ser más susceptibles al diseño engañoso o adictivo y pueden estar más expuestos a interacciones perjudiciales en entornos sociales o multijugador.

A menos que un juego esté clara y demostrablemente dirigido exclusivamente a adultos, todos los actores de la industria deben asumir que habrá NNA presentes y tomar sus decisiones en consecuencia. La puerta de entrada a cualquier juego debe diseñarse con consideraciones apropiadas para la edad. Durante la conceptualización de los sistemas de cuentas, los diferentes actores deben diseñar flujos que respalden el consentimiento parental verificable y/o la determinación de la edad cuando sea necesario[17]. Es una buena práctica probar estos flujos con ensayos de UX simulados durante la preproducción para garantizar su eficacia antes de la implementación.

Además, los creadores, diseñadores y desarrolladores que recluten a menores para pruebas de juego tempranas deben especificar un umbral de edad y crear formularios de consentimiento parental separados con registro verificable, asegurando que estos registros se almacenen junto con el ID de cuenta del probador para la responsabilidad proactiva.

En general, el Artículo 8 del RGPD introduce un requisito adicional: cuando el tratamiento se base en el consentimiento y el sujeto de datos esté por debajo de la edad en la que puede dar un consentimiento válido, la autorización parental debe ser verificable. Un mecanismo de consentimiento parental bien diseñado equilibra dos demandas competitivas: debe ser lo suficientemente fiable para permitir que su validez se verifique con un nivel de certeza suficiente, pero también debe ser proporcional, de modo que no requiera identificación intrusiva. Los enfoques comunes incluyen el envío de un código de verificación de un solo uso a la dirección de correo electrónico de un tutor, el uso de una verificación de tarjeta de

[17] EDPB Statement 1/2025 on Age Assurance, https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

pago *tokenizada* sin almacenar la información de la tarjeta, o el uso de un panel parental que requiera que un tutor apruebe explícitamente la participación del NNA.

IV.D.3 Construcción de interfaces apropiados para la edad

Los Artículos 12, 13 y 14 del RGPD exigen que la información sobre protección de datos se facilite de manera "inteligible y de fácil acceso", con adaptaciones especiales para los NNA. En la práctica, esto implica diseñar interfaces de transparencia que reflejen las capacidades cognitivas de los jugadores. Las explicaciones simplificadas, las ilustraciones visuales, los ejemplos concretos ("Guardamos tu progreso para que no lo pierdas") y una terminología consistente en todos los menús contribuyen a una comprensión adecuada. Cuando se separa por edad, la versión para la experiencia de los NNA debe, por defecto, ajustarse a las recomendaciones aplicables en los códigos de diseño apropiados para su edad. En el caso de la protección por defecto, todos los usuarios son tratados de la misma manera porque se desconoce su edad, ni si superan cierta edad. Los estándares del código deben aplicarse a todos los usuarios, garantizando que los menores estén consistentemente expuestos a un diseño adecuado para ellos.

Esto asegura que sus necesidades sean respetadas y que sus intereses estén protegidos. Los adultos que confirmen su edad pueden modificar esta interfaz o la configuración por defecto. Este enfoque también puede beneficiar a usuarios con menor competencia digital, discapacidades específicas o personas mayores, por mencionar solo algunos ejemplos. Todos los usuarios (no solo los NNA) deben tener la opción de acceder voluntariamente a diferentes versiones de diseño de las interfaces y de los avisos de transparencia según sus necesidades y preferencias. Este diseño adaptativo no tiene necesariamente que basarse en procesos de verificación de edad, sino más bien en ofrecer a los usuarios opciones para elegir libremente las que consideren más adecuadas, útiles o beneficiosas para ellos. El objetivo no es meramente la claridad estética, sino garantizar, por ejemplo, que el consentimiento sea válido si se utiliza como base jurídica.

IV.D.4 Identificación de funcionalidad de alto riesgo para la infancia y protección de los NNA

Ciertas funcionalidades de los juegos conllevan riesgos inherentes elevados cuando son utilizadas por NNA, como los canales de comunicación públicos, los algoritmos de recomendación de amigos, las interacciones basadas en la ubicación, las mecánicas de realidad aumentada con cámara, los avatares identificables y las microtransacciones opacas, como las cajas botín. Los creadores, diseñadores y desarrolladores deben evaluar si estas funcionalidades son compatibles con el interés superior del menor y qué salvaguardas adicionales pueden ser necesarias. La protección de los menores debe integrarse en el diseño y la arquitectura del juego. Los creadores, diseñadores y desarrolladores pueden implementar modos de comunicación restringidos, filtros automatizados, paneles para tutores, límites de gasto, restricciones por hora del día o herramientas de denuncia accesibles. Estas decisiones de diseño refuerzan simultáneamente la protección, la privacidad y el cumplimiento del RGPD.

A nivel de sistema, los *storefronts* y los lanzadores deben planificar la restricción de las cuentas genéricas a las funcionalidades por defecto y desactivar las funcionalidades sociales también por defecto, vinculando estas restricciones directamente a los controles de edad en el modelo de datos. Solo los adultos deben poder cambiar este tipo de configuración segura.

Uno de los casos en los que más aumenta el riesgo para los NNA es la elaboración de perfiles de comportamiento (y en la publicidad asociada). En este sentido, todos los actores

de la industria deben adoptar un enfoque de “protección por defecto”, a menos que el juego esté disponible solo para adultos. Los proveedores de hardware deben desactivar explícitamente la elaboración de perfiles orientada a la monetización para los usuarios genéricos que no demuestren tener una edad superior al umbral requerido. Los proveedores de tecnología para el desarrollo deben diseñar su servicio para aceptar y procesar una señal de edad, de modo que las funcionalidades puedan restringirse o activarse automáticamente en función de la edad verificada, y apoyar esta buena práctica. Los creadores, diseñadores y desarrolladores que incluyan a menores en pruebas de juego deben evitar perfiles que midan o exploten el gasto o la compulsión, limitando su análisis a patrones de usabilidad y frustración que impulsen, estrictamente, mejoras en el diseño.

Los editores deben garantizar que solo las cuentas marcadas como “de adultos” puedan activar la elaboración de perfiles orientada a la monetización. Finalmente, los *storefronts* deben establecer “sin marketing personalizado” como opción por defecto para las cuentas genéricas y asegurarse de que las recomendaciones para estos usuarios se limiten a sugerencias no basadas en perfiles, como las selecciones del editor. En general, para los juegos accesibles a audiencias jóvenes y populares entre ellas, todos los actores deben marcar y revisar activamente cualquier modelo de elaboración de perfiles dirigido a maximizar la monetización o el compromiso, considerando objetivos alternativos (como la satisfacción o el bienestar). Los proveedores de tecnología para el desarrollo deben incluir cláusulas contractuales que prohíban a los clientes pasar etiquetas de “menor” a las API de elaboración de perfiles sin salvaguardas adicionales acordadas.

V. RECOMENDACIONES Y MEJORES PRÁCTICAS EN LA FASE DE LANZAMIENTO

Esta etapa marca el momento en que la filosofía del diseño de un juego se convierte en realidad operativa. Conceptos del RGPD como la determinación de bases jurídicas, la lealtad, la transparencia, la protección de datos por defecto o la protección de los menores, que pueden haber permanecido teóricos durante la preproducción y producción, deben ahora materializarse en la práctica en las interfaces, configuraciones, viajes de usuario, flujos de monetización y sistemas *backend* con los que, potencialmente, millones de jugadores interactuarán. Mientras que la preproducción y la producción requieren imaginación y planificación, la fase de lanzamiento exige disciplina: la disciplina de garantizar que cada funcionalidad, cada elección durante la incorporación de un jugador, cada práctica de recogida de datos y cada interacción se alineen con los compromisos legales y éticos que los responsables y encargados del tratamiento han adoptado.

Las operaciones en vivo añaden una capa adicional de complejidad. Una vez que los jugadores comienzan a interactuar con el juego a gran escala, los estudios se enfrentan a presiones continuas en tiempo real: lanzamiento de funcionalidades, parches de contenido, ciclos de equilibrio de dificultad, normas comunitarias nuevas, comportamientos adversarios, necesidades de automatización, ciberataques y ajustes de las estrategias monetización. El cumplimiento del RGPD no debe simplemente sobrevivir en este entorno, sino que debe permanecer estable y fiable, incluso bajo presiones comerciales o ciclos de desarrollo rápidos.

A. IDENTIFICACIÓN DE ROLES Y RESPONSABILIDADES EN RELACIÓN CON EL RGPD

La identificación de estos roles debería haberse realizado en la primera etapa del ciclo de vida del juego, ya que es una tarea que debe llevarse a cabo durante la fase de preproducción y producción, cuando se planifican todas las actividades de tratamiento de datos personales. Sin embargo, todas las preguntas orientativas sobre el tratamiento que se lleva a cabo una vez que el videojuego está en el mercado se incluyen aquí a modo de clarificación. Quizás algunas de las preguntas orientativas de la sección IV.A también puedan ser útiles a la hora de determinar los roles conforme al RGPD en esta etapa.

V.A.1 Proveedores de hardware

Preguntas de orientación:

- ¿Son obligatorias las cuentas de plataforma para jugar al juego o acceder a funcionalidad en línea, y ¿se establecen campos obligatorios, comprobaciones de seguridad y reglas de vinculación entre dispositivos? Si es así, usted es el responsable del tratamiento de esas cuentas.
- ¿Usted y un desarrollador o editor deciden conjuntamente funcionalidades compartidas entre cuentas (progresión cruzada, lista de amigos unificada, prohibiciones entre títulos)? Si es así, evalúe la corresponsabilidad.
- ¿Ofrece una solución de inicio de sesión que los editores pueden personalizar y configurar, mientras que usted también reutiliza los datos de la cuenta para su propia analítica o marketing? Si es así, usted es responsable independiente por su reutilización; el editor es responsable por su uso, incluso si se utiliza la misma cuenta.

- ¿Recoge telemetría de la plataforma de todos los juegos (tiempo de sesión, rendimiento, informes de errores, patrones de uso) para optimizar la plataforma, hacer cumplir las políticas y recomendar juegos? Si es así, usted es el responsable de ese tratamiento.
- ¿Comparte la telemetría de la plataforma con los editores a través de paneles que codiseñan (KPI compartidos que afectan a las decisiones de ambas partes)? Si es así, examine la corresponsabilidad para ese servicio de analítica compartido.
- ¿Crea perfiles transversales de los hábitos o habilidades de los jugadores en la plataforma de hardware para recomendar títulos o ajustar los umbrales de moderación/antitrampa? Si es así, es responsable del tratamiento de esas inferencias.
- ¿Comparte segmentos (“gran comprador”, “jugador competitivo”) con los editores para sus propias campañas? Si es así, puede tener roles distintos: evalúe si son corresponsables para campañas compartidas o responsables separados que intercambian datos.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuenta de la plataforma de hardware): probablemente responsable del tratamiento, a veces corresponsable o encargado del tratamiento.
- Monitorización del juego (telemetría de plataforma): responsable del tratamiento, corresponsable cuando la telemetría se utiliza conjuntamente con los editores.
- Inferencia de comportamiento (inferencias de plataforma): probablemente responsable del tratamiento.

V.A.2 Creadores, diseñadores y desarrolladores

Preguntas de orientación:

- ¿Expone el juego una interfaz de registro o cuenta en el juego bajo la marca de su estudio, con su propia política de privacidad? Si es así, usted es el responsable del tratamiento de esa cuenta.
- ¿Gestiona cuentas únicamente en nombre de un editor (marca del editor, política de privacidad del editor, el editor decide los campos y la reutilización)? Si es así, usted es el encargado del tratamiento para el tratamiento asociado a esa cuenta.
- ¿Conserva las cuentas de prueba (jugadores de acceso anticipado) hasta el lanzamiento y las reutiliza para la comunidad o analítica? Si es así, usted es el responsable del tratamiento.
- ¿Quién decide qué eventos de telemetría se instrumentan (por ejemplo, finalización de niveles, pulsaciones de botones, eventos de chat) y por qué? Si usted decide o codecide más allá de la necesidad técnica, puede ser responsable o corresponsable del tratamiento.
- ¿Almacenará la telemetría en su propio entorno y la reutilizará en varios títulos para mejorar el diseño, el equilibrio de la dificultad o los modelos de IA? Si es así, es responsable del tratamiento.

- ¿Está contractualmente obligado a recoger y reenviar telemetría en bruto exactamente como especifique el editor, sin reutilización independiente? Si es así, es encargado del tratamiento.
- ¿Diseña o ajusta modelos en vivo para emparejamiento, dificultad dinámica o contenido personalizado directamente en su bucle de operaciones en tiempo real, para sus propios títulos? Si es así, es responsable del tratamiento.
- ¿Implementa lógica de elaboración de perfiles enteramente según lo especificado por el editor, en sus sistemas, sin reutilización entre juegos o clientes? Si es así, probablemente sea encargado del tratamiento.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas del juego): responsable del tratamiento para las cuentas de prueba propias; encargado del tratamiento si las cuentas se gestionan para un editor.
- Monitorización del juego (telemetría del juego): encargado del tratamiento al recopilar telemetría únicamente para el editor, responsable del tratamiento al utilizar datos para su propia I+D en diferentes proyectos.
- Inferencia de comportamiento (inferencias del juego): responsable del tratamiento al crear modelos para sus propios fines, encargado del tratamiento al crear modelos únicamente para el editor bajo instrucciones.

V.A.3 Proveedores de tecnología para el desarrollo

Preguntas de orientación:

- Cuando los jugadores inician sesión con su servicio de gestión de identidad (por ejemplo, una cuenta vinculada al motor de desarrollo), ¿establece usted los términos de uso y reutiliza los datos en varios juegos? Si es así, es el responsable del tratamiento asociado a esa cuenta.
- Si un editor exige que se use su servicio de gestión de identidad, pero le prohíbe reutilizar los datos y usted trabaja estrictamente bajo sus instrucciones documentadas, ¿se limita a la autenticación desde el punto de vista técnico? Si es así, puede actuar como encargado del tratamiento para ese tratamiento específico.
- ¿Envía su servicio automáticamente datos de telemetría a sus servidores desde cada juego en directo (por ejemplo, rendimiento, información del dispositivo, detalles de fallos) para mejorar su producto e investigar? Si es así, es el responsable de ese tratamiento.
- ¿Pueden los estudios configurar la telemetría para que se mantenga completamente local o vaya solo a un punto final (*end point*) gestionado por ellos? Si eligen su punto final, pero usted reutiliza agregados de alto nivel entre clientes, sigue actuando como responsable del tratamiento de esa reutilización.
- ¿Proporciona una pila de análisis alojada en su infraestructura en la que el editor define eventos, métricas, plazos de conservación, y usted está contractualmente obligado a no reutilizar los datos? Si es así, puede ser el encargado del tratamiento para esa pila.
- ¿Ofrece servicios genéricos de predicción de abandono, compromiso o monetización en varios juegos, entrenados con datos de múltiples clientes? Si es así, es el responsable del tratamiento de ese perfilado, incluso si los estudios también son responsables del tratamiento al aplicar las predicciones obtenidas.

- ¿Definen usted y clientes específicos, de manera conjunta, los criterios de segmentación y las reglas de campañas utilizando su motor? Si es así, evalúe si hay corresponsabilidad del tratamiento.
- ¿Se limita a proporcionar un entorno alojado en el que el cliente sube datos, define modelos, y usted ni accede a, ni reutiliza los datos? En ese caso, para esa actividad puede estar más cerca de ser el encargado del tratamiento o incluso fuera del ámbito de responsable/encargado del tratamiento en lo que respecta a los datos de los usuarios finales.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas propias del servicio): responsable del tratamiento; encargado del tratamiento si se limita a autenticar para un cliente.
- Monitorización del juego (telemetría del servicio): a menudo responsable del tratamiento, a veces corresponsable del tratamiento; puede ser encargado del tratamiento si está realmente sujeto a instrucciones.
- Inferencia conductual (inferencias del servicio): responsable del tratamiento para modelos conductuales genéricos (posible corresponsable del tratamiento), a veces encargado del tratamiento.

V.A.4 Editores

Preguntas de orientación:

- ¿Gestiona cuentas de editor que conectan varios juegos, plataformas y dispositivos, y define todos los fines (análisis entre títulos, ofertas, bloqueos)? Si es así, es el responsable del tratamiento.
- ¿Los programas de fidelización, la progresión entre juegos o las listas de bloqueo combinadas se codiseñan con plataformas o *storefronts*? Si es así, determine si hay corresponsabilidad del tratamiento o si son responsables del tratamiento independientes que intercambian datos (depende de la arquitectura y los flujos de datos).
- ¿Define KPIs en directo (abandono, dificultad, monetización, toxicidad) y decide qué eventos de telemetría envía cada versión del juego a los servidores en tiempo real? Si es así, es el responsable del tratamiento.
- ¿Combina la telemetría de la plataforma, la telemetría del *storefront* y la telemetría dentro del juego en vistas unificadas de los jugadores? Si es así, claramente es el responsable del tratamiento.
- ¿Depende de paneles de control de proveedores en los que tanto usted como el proveedor deciden qué segmentos o desencadenantes utilizar (por ejemplo, promociones basadas en el comportamiento en tiempo real)? Si es así, considere si hay corresponsabilidad del tratamiento.
- ¿Desarrolla o encarga modelos para segmentar jugadores con el fin de adaptar ofertas, eventos, dificultad o estrategias de retención? Si es así, es el responsable del tratamiento.
- ¿Estos modelos se codiseñan con plataformas o *storefronts* (por ejemplo, *retargeting* conjunto)? Si es así, examine si hay corresponsabilidad del tratamiento para ese programa específico.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas del editor): responsable del tratamiento; a veces corresponsable del tratamiento junto con creadores, diseñadores y desarrolladores.
- Monitorización del juego (telemetría del editor): responsable del tratamiento de la telemetría; corresponsable del tratamiento con otros actores cuando deciden conjuntamente.
- Inferencia conductual (inferencias del editor): responsable del tratamiento del perfilado basado en el juego; a veces corresponsable del tratamiento con proveedores de hardware/proveedores de tecnología para desarrollo/*storefronts*.

V.A.5 *Storefronts*

Preguntas de orientación:

- ¿Son obligatorias las cuentas del *storefront*/lanzador para usar funcionalidad social, realizar compras y guardar en la nube, y las reutiliza en varios juegos? Si es así, es el responsable del tratamiento.
- ¿Existen "centros de editores" de marca compartida en los que usted y un editor codeterminan los criterios de membresía y los beneficios (por ejemplo, niveles VIP en diferentes juegos)? Si es así, evalúe si hay corresponsabilidad del tratamiento asociado a ese club o comunidad.
- ¿Realiza un seguimiento de los juegos instalados, la frecuencia de juego, la duración de las sesiones, la navegación en el lanzador y las compras para mejorar el *storefront* y personalizar las recomendaciones? Si es así, es el responsable del tratamiento.
- ¿Proporciona a los editores acceso a la telemetría del *storefront* (impresiones, clics, conversiones) que ambos utilizan para optimizar las promociones? Esto puede seguir siendo una responsabilidad del tratamiento independiente, pero la segmentación diseñada de manera conjunta puede indicar corresponsabilidad del tratamiento para esa promoción.
- ¿Perfila a los jugadores en función de las compras, las listas de deseos, el tiempo de juego y la navegación para recomendar juegos y mostrar ofertas? Si es así, es el responsable del tratamiento.
- ¿Realiza campañas conjuntas en las que usted y un editor codeterminan la regla de segmentación (por ejemplo, "mostrar este lote de juegos al segmento X en el momento Y") utilizando datos compartidos? Si es así, probablemente haya corresponsabilidad del tratamiento para esa campaña.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuenta del *storefront*): responsable del tratamiento; posiblemente corresponsable del tratamiento con editores para programas de marca compartida.
- Monitorización del juego (telemetría del *storefront*): responsable del tratamiento de la telemetría utilizada para gestionar y optimizar el *storefront*/lanzador; corresponsable del tratamiento si determina la telemetría junto con los editores.

- Inferencia conductual (inferencias del *storefront*): responsable del tratamiento de sus propios sistemas de recomendación y publicidad dirigida; a veces corresponsable del tratamiento con editores para campañas conjuntas.

B. PROTECCIÓN DE LOS DATOS PERSONALES MIENTRAS SE JUEGA

V.B.1 Integración de la transparencia en la experiencia de juego

Cuando los jugadores inician un juego por primera vez, deben poder entender, en términos claros y contextualizados, cómo se tratarán sus datos personales. Los Artículos 12, 13 y 14 del RGPD exigen que la información sea concisa, inteligible y de fácil acceso, pero no imponen un formato o forma específicos en los que deba proporcionarse. Los juegos, por tanto, tienen un enorme margen creativo para integrar la transparencia en la experiencia del jugador, en lugar de relegarla a textos legales estáticos ocultos en diferentes políticas de privacidad y ubicaciones.

Un flujo bien diseñado introduce los conceptos de privacidad de manera gradual. Esto suele comenzar con una explicación breve y comprensible de la información básica: se tratarán ciertos datos personales para crear una cuenta o permitir la progresión, las funcionalidades opcionales pueden requerir permisos adicionales, los jugadores pueden revisar y cambiar su configuración de privacidad en cualquier momento posterior. Al integrar la transparencia en el ritmo natural de los procesos de incorporación al juego en lugar de interrumpirlos, los diferentes actores del ecosistema evitan abrumar a los jugadores y, al mismo tiempo, respetan sus derechos.

Existe la posibilidad de crear etiquetas de privacidad que desempeñen para los tratamientos de datos el mismo papel que PEGI[18] para el contenido de los juegos: una señal estandarizada y visible que, de un vistazo, ayude a las personas a tomar decisiones más rápidas y mejor informadas en el momento exacto de la elección (páginas del *storefront*, pantallas de instalación, solicitudes de actualización, etc.). PEGI ya ha demostrado que el ecosistema de los videojuegos puede utilizar con éxito un formato compacto, codificado por colores y ampliamente reconocido para simplificar información de riesgo compleja para jugadores y padres. En general, se recomiendan metodologías de presentación simplificadas y visuales. En particular, los responsables del tratamiento deben tener en cuenta las especificidades de los dispositivos utilizados para jugar y de las interfaces, por ejemplo, en lo que respecta a las limitaciones de espacio disponible. Las etiquetas de privacidad no sustituirían a las políticas completas, al igual que PEGI no describe todos los aspectos de un juego. Más bien, la etiqueta funcionaría como una capa inicial de transparencia, mientras que la información detallada subyacente seguiría disponible para los jugadores que la deseen.

En este sentido, los mecanismos de transparencia más efectivos anticipan el contexto. Por ejemplo, si un jugador intenta activar el chat de voz por primera vez, la información de transparencia relevante debe aparecer de inmediato, en lugar de estar oculta en un menú. Asimismo, si el juego ofrece recomendaciones personalizadas o eventos basados en la ubicación, la interfaz debe explicar qué datos se requieren y por qué en el momento en que la funcionalidad se vuelve relevante. La transparencia, por tanto, se convierte en un diálogo continuo en lugar de ser una notificación puntual que suele ignorarse y luego olvidarse.

[18] PEGI (*Pan European Game Information*) es el sistema europeo armonizado y centralizado de clasificación por edades para videojuegos. Utiliza categorías de edad y descriptores de contenido para ayudar a los jugadores y a los padres a comprender rápidamente si un juego es adecuado y qué tipo de contenido incluye, https://pegi.info/

Además, es recomendable vincular cada elemento de datos a su base jurídica (contrato para el identificador principal, intereses legítimos para las señales de fraude, consentimiento para las señales de marketing, etc.) al implementar este tipo de aviso de privacidad "en directo". Utilice un lenguaje claro en los mensajes, pantallas e interfaces (por ejemplo: "Necesitamos su correo electrónico para guardar las partidas: el tratamiento es necesario para la ejecución de un contrato") y siempre proporcione enlaces a la información de privacidad por capas.

Los actores que interactúan con mayor frecuencia y de manera más explícita con los jugadores, como editores o *storefronts* (así como ciertos proveedores de hardware), deben implementar centros o sitios de privacidad dedicados para agrupar toda la información, los mecanismos de transparencia y las herramientas asociadas (véase la sección V.C más adelante). La colaboración entre los diferentes actores del ecosistema es necesaria para garantizar que los jugadores dispongan de información clara sobre "quién es quién". Los mecanismos de transparencia deben cubrir explícitamente la tecnología, los juegos y las integraciones de plataformas, e identificar a los responsables del tratamiento en patrones típicos (por ejemplo, para los datos de la cuenta: "Cuando usa su cuenta en X para iniciar sesión en el Juego ofrecido por Y, X es el responsable del tratamiento de datos asociados a su cuenta e Y es el responsable del tratamiento de sus datos del juego"). Evite expresiones vagas como "socios de confianza" y proporcione a los jugadores información clara para que comprendan qué datos se compartirán, con qué fin y con qué base jurídica. Cree y publique catálogos de telemetría, que incluyan información sobre eventos, campos, destinatarios y usos.

Las cajas botín y otras mecánicas basadas en el azar se han convertido en un foco regulatorio en Europa. Cuando estas mecánicas impliquen el tratamiento de datos personales, las obligaciones de transparencia exigen que se informe a los jugadores, por ejemplo, de la probabilidad de recibir diferentes recompensas, y esta información debe presentarse antes de una compra, no ocultarse en una política remota o de difícil acceso. Si las probabilidades cambian dinámicamente (por ejemplo, si aumenta la probabilidad de obtener recompensas raras tras compras repetidas), debe informarse de esto al jugador.

V.B.2 Obtención de consentimiento válido

En el lanzamiento, los responsables del tratamiento deben implementar mecanismos de consentimiento robustos y dirigidos a los jugadores, que cumplan los requisitos para un consentimiento válido conforme a los Artículos 4(11) y 7 del RGPD. El consentimiento válido implica un consentimiento que sea libre, específico, informado e inequívoco. Estos mecanismos de consentimiento actúan como la puerta de entrada crítica para todo el tratamiento de datos personales que se fundamenta en esta base jurídica. Esta etapa del ciclo de vida del juego marca el tono para la confianza y el cumplimiento, y requiere *banners* granulares y desglosados que se presenten antes de que comience el juego, con explicaciones claras sobre la recolección de telemetría, el perfilado y el intercambio con terceros, vinculados a fines específicos como la analítica, las funcionalidades sociales o la monetización. Nuevamente, los mensajes, menús e interfaces deben adaptarse para que las ventanas sean legibles en diferentes dispositivos y entornos, prestando especial atención a los posibles problemas de accesibilidad.

Los responsables del tratamiento deben utilizar acuerdos de aceptación durante la incorporación (*clickwraps*) para bloquear la progresión hasta que se recojan los consentimientos, basándose en avisos por capas. Por ejemplo, "Alta recolección de telemetría: sesiones y entradas se comparten con 3 socios publicitarios", seguido de detalles ampliables sobre los flujos de datos y los derechos de retirada del consentimiento. Las opciones deben presentarse de manera granular y equilibrada, con selectores separados

para cada categoría. Por ejemplo, “Analítica (esencial)”, “Anuncios personalizados (opcional)”, “Perfilado entre títulos (si te apuntas)”. Asegúrese de que “Rechazar todos” sea tan destacado y sencillo como “Aceptar”, sin que esto implique denegar las funciones principales del juego. Proporcione contexto y permita a los jugadores previsualizar las consecuencias, evitando la jerga y evaluando la comprensión mediante estudios de usabilidad. Por ejemplo, “Esta opción permite la recomendación de botines basada en tu estilo de juego—tus datos personales se almacenan en local excepto si consientes a que se compartan”.

Los responsables del tratamiento pueden recurrir a diferentes mecanismos para mantener al jugador informado de manera proactiva. Por ejemplo, las notificaciones dentro del juego pueden utilizarse para activar ventanas emergentes o *banners* ante cambios en la configuración (por ejemplo, al cambiar de compartir de forma privada por defecto a pública), nuevas funcionalidades que recojan telemetría (por ejemplo, “Esta actualización añade perfilado de comportamiento para anuncios personalizados—¿revisar/rechazar?”), o monetización basada en inferencias (por ejemplo, inducción a las cajas botín). Las alertas *push* también pueden ser útiles para enviar notificaciones al dispositivo en caso de eventos de alto riesgo, como el intercambio de datos de la cuenta con tecnología publicitaria de terceros o los impactos en la privacidad tras una actualización, con opciones de deshacer con un solo toque. Las advertencias integradas permiten a los diferentes actores incluir indicadores en tiempo real durante el juego o en los menús, por ejemplo, “Estás activando el chat de voz y para ellos se comparten datos obtenidos con el micrófono—¿confirmas?” o “La instalación de este contenido descargable modifica los tiempos de retención de tu analítica—detalles”.

Finalmente, los responsables del tratamiento pueden ofrecer registros de las modificaciones relativas al tratamiento de datos personales accesibles para el usuario y visibles en tiempo real (por ejemplo, “Cambio de configuración 10:56 AM CET: telemetría activada”), exportables para su portabilidad. Además, los responsables del tratamiento deben registrar todas las interacciones (marca de tiempo, identificador del dispositivo, decisiones tomadas) en registros a prueba de manipulaciones con fines de auditoría, teniendo en cuenta el principio de responsabilidad proactiva (Artículo 5(2) del RGPD). También deben activar el registro del consentimiento de los padres para los probadores menores de edad, los jugadores de acceso anticipado y el resto de los jugadores por debajo de la edad límite que aplique en cada caso.

V.B.3 Limitación de la finalidad y minimización de datos durante el tiempo de juego

Todos los actores que participan en el ecosistema deben crear un esquema o diccionario de cuentas actualizado y ejecutar *scripts* de verificación para garantizar que se actualice correctamente. Los campos sociales deben ser de adhesión voluntaria (*opt-in*) durante la incorporación de los jugadores al juego, y los campos de perfil de texto libre deben reemplazarse por vocabularios controlados (menús desplegables, casillas de verificación). Los responsables del tratamiento deben configurar la eliminación automática de cuentas inactivas tras un período fijo (activada por la marca de tiempo del último inicio de sesión), siempre con notificación previa al jugador (por ejemplo, mediante un correo electrónico a la dirección vinculada a la cuenta). También deben implementar procedimientos automatizados y granulares de conservación, por ejemplo, datos principales de la cuenta durante 5 años después del último inicio de sesión, datos de marketing durante 12 meses a menos que se renueve el consentimiento. En general, se recomienda ejecutar periódicamente *scripts* de verificación para garantizar que todas las medidas planificadas de protección de datos desde el diseño y por defecto se implementen correctamente tras el lanzamiento.

Durante el juego, los datos personales se generan de manera continua. Incluso en juegos sencillos, la telemetría y las inferencias constituyen fuentes ricas de datos personales. En entornos multijugador complejos, el volumen y la granularidad de los datos son aún mayores. El principio de limitación de la finalidad del Artículo 5(1)(b) exige que este flujo continuo de datos esté vinculado a los fines específicos y explícitos identificados en la fase de preproducción y producicón. Los responsables de estas actividades de tratamiento deben bloquear un esquema o lista blanca de telemetría e inferencias, aplicar este esquema predefinido y rechazar actualizaciones o parches que añadan eventos o atributos no documentados o arbitrarios. También deben limitar explícitamente las ventanas de perfil (el intervalo de tiempo durante el cual esa telemetría es utilizada para crear o actualizar las inferencias) e implementar procedimientos automatizados de conservación, diferenciando entre datos en bruto, inferencias o perfiles, y agregados. Finalmente, deben intentar podar periódicamente los esquemas de datos, simplificando o recortando sus conjuntos de datos personales mediante la eliminación de elementos innecesarios, redundantes o no utilizados, como campos, atributos o inferencias.

En lo que respecta al principio de minimización de datos, es recomendable revisar periódicamente diversos aspectos de cualquier actividad de tratamiento, como el volumen, la precisión y la frecuencia de la recolección de telemetría, frente a las necesidades reales de su finalidad declarada. Los responsables del tratamiento deben realizar una comprobación de finalidad-necesidad, documentando si la recolección de determinados datos personales es necesaria para la finalidad declarada.

La tentación de explotar los datos del juego para nuevos fines crece rápidamente una vez que un juego tiene éxito comercial. Diferentes actores pueden desear reutilizar la telemetría recogida originalmente para depuración con el fin de crear funcionalidades y ofertas personalizadas; los equipos de producto pueden querer analizar patrones conductuales para predecir la retención. Sin embargo, como se ha discutido anteriormente, a menos que el aviso de transparencia original anticipara estos usos o que una evaluación de compatibilidad conforme al Artículo 6(4) los respalde, los responsables del tratamiento deben identificar una nueva base jurídica. Sin este paso, la reutilización de datos se convierte en ilícita.

V.B.4 Alineamiento de las mecánicas de monetización y los principios del RGPD

Los responsables del tratamiento deben distinguir claramente entre los datos estrictamente necesarios para el juego y los datos utilizados para optimizar la monetización (ofertas personalizadas, segmentación de grandes gastadores, audiencias similares), que, en la práctica, suelen requerir un consentimiento granular y de adhesión voluntaria (*opt-in*). Si el juego genera ofertas dirigidas o precios dinámicos basados en el comportamiento pasado, los datos que respaldan estas decisiones deben recogerse y tratarse de conformidad con la ley. Además, se recomienda registrar explícitamente cada caso en el que los usuarios (o dispositivos) se clasifiquen en segmentos conductuales basados en telemetría o inferencias.

Los modelos de monetización, como las microtransacciones, los niveles de suscripción, las economías virtuales o las ventas de elementos cosméticos, deben ser compatibles con los principios del RGPD, en particular la lealtad y la transparencia conforme al Artículo 5. Los responsables del tratamiento deben evitar mecánicas que realicen un seguimiento de la frustración o los sesgos cognitivos o que intenten explotar debilidades específicas; esto puede caracterizarse como perfilado manipulativo (relacionado con los patrones de diseño adictivo) en lugar de un tratamiento de datos leal. El diseño de la monetización no debe basarse en un perfilado psicológico opaco que los jugadores no esperen o comprendan razonablemente, en particular cuando afecta a menores y grupos vulnerables.

Los responsables del tratamiento deben ir más allá del lenguaje genérico “mejoramos nuestros servicios” y explicar, en términos sencillos, qué telemetría se recoge (eventos, datos de sesión, dispositivo, grafo social), qué inferencias de monetización se extraen (por ejemplo, riesgo de abandono, propensión a gastar mucho, vulnerabilidad de compromiso excesivo) y cómo se utilizan.

Deben evitar desvirtuar la finalidad del tratamiento. Por ejemplo, un estudio podría analizar el compromiso de un jugador con un modo de juego concreto y, a continuación, ofrecer un objeto cosmético único relacionado con ese modo. Si los datos personales utilizados para generar esa oferta se recogieron originalmente únicamente para equilibrar la dificultad del juego, su reutilización con fines de monetización puede ser ilícita sin un consentimiento válido.

Además, la telemetría recogida inicialmente para seguridad o calidad no debe reutilizarse silenciosamente en perfiles de monetización entre títulos o dispositivos, especialmente cuando se comparte entre los actores del ecosistema. Debe implementarse una separación contractual y técnica: la telemetría de hardware/sistema operativo, la telemetría de juego y la analítica del *storefront* deben estar aislados, con acuerdos explícitos e interfaces auditables cuando los datos se combinen para monetización.

Los responsables del tratamiento deben utilizar la telemetría mínima necesaria para alcanzar un objetivo de monetización concreto (por ejemplo, el historial de gastos recientes y la progresión aproximada, en lugar de flujos de clics completos, cronologías detalladas o comunicaciones en bruto). Además, deben limitar la ventana temporal de los datos utilizados para las inferencias de monetización (por ejemplo, las últimas sesiones en lugar de todo el historial) y agrupar los datos cuando sea posible; esto reduce la identificabilidad y la profundidad de la explotación conductual. Deben evitar inferencias sensibles innecesarias, como derivar o almacenar atributos asociados a la probabilidad de adicción, el estado de salud mental o el estrés financiero únicamente para optimizar los ingresos.

Por otro lado, las inferencias conductuales en la monetización (por ejemplo, el riesgo de abandono o el estado de “alto valor”) no deben tratarse como verdades estáticas. Los responsables del tratamiento deben implementar mecanismos para la actualización periódica de modelos y la comprobación de sesgos, por ejemplo.

Los responsables del tratamiento también deben supervisar y regular activamente la colocación de productos (objetos de marca integrados), los anuncios dinámicos (*banners* personalizados, cajas botín) y los patrocinios (eventos de marca, aspectos visuales) para evitar un tratamiento desleal. También es una buena práctica fomentar el bienestar de los jugadores incorporando puntos de control, guardados automáticos y pausas naturales (temporizadores de sesión, solicitudes de “descanso sugerido”) para limitar el exceso de participación o compromiso.

C. FACILITACIÓN DEL EJERCICIO DE DERECHOS A TRAVÉS DE INTERFACES CENTRADAS EN EL JUGADOR

V.C.1 Ejercicio sencillo de los derechos del interesado

Los actores que participan en el ecosistema deben mantener una matriz de roles por tipo de cuenta (cuenta de desarrollador, cuenta de probador, cuenta de jugador, etc.) y actividad de tratamiento de datos que especifique quién es el responsable/corresponsable del tratamiento y quién responde a las solicitudes de derechos de los interesados. Sin embargo, el ejercicio de los derechos de los interesados conforme al RGPD solo puede ser efectivo

cuando es accesible, inteligible e integrado en los mismos entornos en los que los interesados (jugadores) toman decisiones sobre sus datos personales. En muchos servicios digitales que no son juegos, los derechos se ejercen mediante formularios web o solicitudes por correo electrónico. En el contexto de un videojuego, sin embargo, estos enfoques pueden resultar desconectados de la experiencia, lentos o inaccesibles, en particular para los jugadores que interactúan principalmente con el juego a través de consolas o dispositivos móviles en lugar de mediante una interfaz web.

Por esta razón, los responsables del tratamiento deben considerar los derechos de los interesados como un componente central del diseño de la experiencia del jugador. Una interfaz de derechos debe estar ubicada en la configuración de la cuenta o en una sección claramente marcada como “privacidad” o “gestión de datos personales” dentro del menú principal. No debe estar oculta tras múltiples capas de menú ni requerir navegar a sitios web externos. Lo ideal es que los jugadores puedan acceder a la gestión de derechos en todas las plataformas en las que el juego esté disponible, incluidos PCs, consolas y dispositivos móviles. Incorporar los derechos en interfaces familiares y nativas del juego evita fricciones innecesarias. Además, refuerza los principios de lealtad y transparencia de los artículos 5(1)(a) y 12 del RGPD al garantizar que los jugadores no se sienten intimidados o excluidos de ejercer sus derechos simplemente porque los mecanismos para hacerlo estén ocultos o sean difíciles de encontrar, acceder o utilizar.

Los proveedores de tecnología para el desarrollo deben respaldar el ejercicio de los derechos de los interesados exponiendo todas las APIs necesarias para acceder, rectificar, etc. los datos personales en sus diferentes ubicaciones. Además, los responsables del tratamiento deben implementar sistemas de *tickets* de soporte al cliente para dar apoyo a las solicitudes de ejercicio de derechos de los interesados y realizar pruebas de extremo a extremo con cuentas ficticias antes del lanzamiento.

V.C.2 Derecho de acceso (Artículo 15)

El derecho de acceso faculta a los jugadores para obtener confirmación de si sus datos se están tratando y, en ese caso, para recibir una copia de dichos datos, junto con información sobre los fines, las categorías, los plazos de conservación y los destinatarios[19]. Aunque las solicitudes de acceso puedan parecer sencillas, en teoría, los videojuegos generan datos inusualmente ricos y heterogéneos para cada jugador. Junto a los tipos más directos de datos personales, como nombres o direcciones de correo electrónico, la telemetría, los registros de comunicación, los historiales de comportamiento, las clasificaciones de emparejamiento, los estados de progresión, los registros de transacciones y los resultados de moderación probablemente entrarán todos dentro del ámbito de los datos personales.

Por esta razón, los responsables del tratamiento deben diseñar cuidadosamente sus procedimientos de acceso. Una solicitud de acceso no debe generar un volcado abrumador o ininteligible de registros técnicos en bruto que se entregue al jugador. En su lugar, la respuesta debe estar estructurada y ser comprensible, con contexto explicativo cuando sea necesario. Una interfaz de derechos bien implementada puede permitir a los jugadores descargar archivos de datos estructurados directamente desde la configuración de su cuenta, acompañados de descripciones narrativas que expliquen cada conjunto de datos. Cuando los archivos sean demasiado grandes o complejos, la interfaz puede proporcionar resúmenes con la opción de solicitar exportaciones completas mediante un proceso

[19] EDPB Guidelines 01/2022 on data subject rights - Right of access, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en

supervisado. El objetivo no es solo el cumplimiento legal, sino permitir que los jugadores comprendan de manera real qué está ocurriendo con sus datos personales y cómo esto configura su experiencia de juego. Por ejemplo, los editores también deben proporcionar controles sencillos dentro del juego para acceder a las categorías de perfil, al menos a un nivel general.

V.C.3 Derecho de rectificación (Artículo 16)

Ya se ha hecho referencia en este documento a las amenazas y riesgos asociados al tratamiento de datos personales incompletos o inexactos. El derecho de rectificación permite a los jugadores que los datos personales incompletos o inexactos que se estén tratando por parte del responsable del tratamiento sean corregidos. En el contexto de un videojuego, esto suele aplicarse a los detalles de la cuenta, la información del perfil, los nombres para mostrar, la información demográfica (cuando se recoge) o los registros inexactos de acciones dentro del juego. También puede aplicarse cuando una clasificación algorítmica (como una puntuación de habilidad, una puntuación de comportamiento o una señal de toxicidad) contenga errores demostrables.

Los responsables del tratamiento deben diseñar sistemas que puedan responder a las solicitudes de rectificación sin comprometer la integridad del juego ni abrir vías para el abuso. Por ejemplo, un sistema de clasificación competitiva puede basarse en métricas de rendimiento que no puedan simplemente “corregirse”, pero si los datos de progresión de un jugador se han corrompido o se han atribuido incorrectamente, debe existir un procedimiento de rectificación. Debe proporcionarse a los jugadores una orientación clara sobre qué datos pueden y no pueden rectificarse, y por qué.

Para los menores, la rectificación se vuelve especialmente importante. Un menor puede basarse en suposiciones inexactas sobre el significado de las entradas de datos o puede proporcionar involuntariamente información de cuenta incorrecta; por lo tanto, los mecanismos de rectificación deben ser accesibles, sencillos y estar acompañados de texto explicativo.

V.C.4 Derecho de supresión (Artículo 17)

La supresión de datos es uno de los derechos más ejercidos entre los jugadores. El Artículo 17 del RGPD otorga a los interesados el derecho a que sus datos personales sean suprimidos en determinadas circunstancias. Leído en conjunto con el Artículo 12 del RGPD, exige que la supresión sea sencilla, accesible y sin fricciones innecesarias. En los juegos, la supresión suele afectar a conjuntos de datos complejos relacionados con la progresión, los grafos sociales, las compras y los inventarios. No obstante, la obligación legal sigue siendo clara: si un jugador desea eliminar sus datos y no existe ninguna base jurídica que exija su conservación continuada, el responsable del tratamiento debe cumplir.

El derecho de supresión obliga a un responsable del tratamiento que haya compartido datos con otras partes a informar a los demás responsables que tratan esos datos para que supriman cualquier enlace, copia o réplica. El responsable del tratamiento debe adoptar medidas razonables para notificar a estos responsables la solicitud del interesado. Un proceso de supresión respetuoso comienza con claridad. Los jugadores deben ser informados, en un lenguaje claro, sobre lo que ocurrirá cuando se supriman sus datos: si su progresión se perderá de forma permanente, si sus comunicaciones se eliminarán o anonimizarán, si los historiales de compra deben conservarse temporalmente por razones legales, y si algunos elementos (por ejemplo, transacciones irreversibles dentro del juego)

no pueden deshacerse. En cualquier caso, los jugadores también deben ser informados sobre si se conservarán determinadas categorías de datos personales tras cumplir con la solicitud de supresión.

La supresión no debe exigir a los jugadores que contacten con soporte al cliente, expliquen sus motivos o pasen por múltiples pasos de confirmación. En principio, debe ser tan sencilla como la creación de la cuenta en sí. Para los menores y sus tutores debe estar disponible la posibilidad de iniciar la supresión mediante un panel de control parental, en cumplimiento del requisito del Artículo 8 de que el consentimiento, y en consecuencia también su retirada, permanezcan bajo su control.

Los proveedores de tecnología para el desarrollo tienen un papel esencial para ejercer este derecho concreto, ya que deben exponer una o varias APIs para que los clientes puedan enviar solicitudes de supresión de jugadores que afecten a los conjuntos de datos de telemetría e inferencias conductuales.

V.C.5 Derecho a la limitación del tratamiento (Artículo 18)

La limitación suele malinterpretarse o pasarse por alto, pero puede desempeñar un papel crucial en sistemas interactivos como los videojuegos. Un jugador puede solicitar que se limite una actividad de tratamiento concreta cuando impugne la exactitud de sus datos, cuando la actividad de tratamiento sea ilícita, pero prefiera la restricción a la supresión, o cuando los responsables del tratamiento ya no necesiten los datos, pero el jugador necesite que se conserven, por ejemplo, para futuras reclamaciones legales.

En el contexto de un videojuego, la limitación puede detener temporalmente la analítica no esencial, pausar las evaluaciones automatizadas para moderación o suspender ciertos procesos de perfilado conductual mientras se resuelve una disputa. Los responsables del tratamiento deben diseñar mecanismos internos para marcar y aislar los datos cuyo tratamiento se limita y evitar su uso involuntario en las operaciones en curso.

La limitación también desempeña un papel importante en la protección de los jugadores que consideren que han sido clasificados incorrectamente por sistemas automatizados, como los modelos de detección de trampas o de toxicidad. Suspender temporalmente los resultados obtenidos de manera automatizada mientras se revisan los datos subyacentes se alinea tanto con los derechos del interesado como con el principio de lealtad.

V.C.6 Derecho a la portabilidad (Artículo 20)

El derecho a la portabilidad permite a los jugadores obtener sus datos personales en un formato estructurado, de uso común y legible por máquina, así como transmitirlos a otro responsable del tratamiento, al menos cuando el tratamiento se base en el consentimiento o en un contrato (por ejemplo, creación de cuentas, compras dentro del juego). Este derecho se aplica a los datos facilitados por el jugador, como nombres de usuario, correos electrónicos, listas de amigos, listas de reproducción/favoritos, historial de compras, configuraciones de juego, registros de actividad (por ejemplo, logros desbloqueados, tiempo de juego por nivel), telemetría en bruto y contenido generado por el usuario, como clips o perfiles compartidos. Puede no aplicarse a las inferencias (por ejemplo, perfiles conductuales como “riesgo de abandono”), a los datos de terceros o al contenido no personal, como archivos de guardado, a menos que estén vinculados de manera única a una actividad identificable.

Aunque la migración directa entre ecosistemas de juegos sea poco común en la práctica, la portabilidad puede seguir cumpliendo funciones importantes. Por ejemplo, los jugadores

pueden querer exportar sus registros de progresión, datos históricos de partidas, inventarios de elementos cosméticos o grafos sociales para usarlos en aplicaciones complementarias, herramientas comunitarias o plataformas de analítica de *e-sports*. La transferencia directa solo es obligatoria si es técnicamente factible (por ejemplo, compatibilidad de APIs entre plataformas); los responsables del tratamiento deben proporcionar, dentro de sus posibilidades, formatos de exportación bien estructurados con metadatos descriptivos y documentación que explique cómo pueden interpretarse los archivos. Se recomienda proporcionar una descripción explícita de los datos portables, la implementación de botones "exportar mis datos" con vistas previas en formatos comunes, la prueba de transferencias directas para los principales *storefronts*, el uso de plazos de conservación breves para los registros en bruto a fin de simplificar las exportaciones y la coordinación mediante contratos (los editores deben garantizar que los *storefronts* o los desarrolladores propaguen las solicitudes en toda la pila, etc.).

Una portabilidad implementada correctamente fomenta la apertura en el ecosistema de los videojuegos y respeta la autonomía de los jugadores que invierten años en sus "personas" digitales. Debe aclararse que la portabilidad no borra datos ni anula los derechos de propiedad intelectual o las condiciones de licencia.

V.C.7 Derecho de oposición (Artículo 21)

El derecho de oposición es especialmente importante en el sector de los videojuegos porque se aplica al tratamiento que se base en el interés legítimo como base jurídica, que suele incluir el tratamiento con fines como la analítica, la personalización y el modelado conductual relacionado con la seguridad. Cuando un jugador se opone, el responsable del tratamiento debe cesar el tratamiento a menos que pueda demostrar motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del jugador, o a menos que el tratamiento sea necesario para resolver reclamaciones legales.

En la práctica, este derecho puede desempeñar un papel vital en sistemas opcionales como funciones y ofertas personalizadas, esfuerzos de retención dirigidos, motores de recomendación y perfilado entre juegos. Si un jugador se siente incómodo con una telemetría o inferencias conductuales específicas, el juego debe permitirle rechazarlas mediante una interfaz intuitiva, tras lo cual el tratamiento debe cesar a menos que esté justificado por una excepción clara. Los editores y *storefronts* pueden implementar un registro central de exclusión voluntaria que bloquee la telemetría o las inferencias conductuales en todos sus títulos, con opciones de exclusión voluntaria que persistan tras las reinstalaciones.

La oposición por diseño debe estar integrada en las mecánicas del juego. Las funcionalidades específicas del juego deben concebirse como componentes modulares. Por ejemplo, un "motor de reglas" para aplicar perfiles y adaptar la dificultad debe diseñarse de modo que, si un jugador se opone al perfilado, la mecánica pueda desactivarse sin afectar al juego principal.

Los responsables del tratamiento no deben interpretar las oposiciones como simples preferencias. Conforme al Artículo 21, tienen fuerza legal. Por lo tanto, el diseño de las interfaces debe evitar la tentación de disuadir a los jugadores de oponerse, en particular mediante patrones de diseño engañosos.

V.C.8 Decisiones individuales automatizadas, incluida la elaboración de perfiles, en entornos en vivo

Conforme al Artículo 22 del RGPD, los jugadores tienen derecho a no ser objeto de decisiones basadas únicamente en un tratamiento automatizado que produzcan efectos significativos en ellos, a menos que se cumplan ciertas condiciones. Debe tenerse en cuenta que muchas funciones principales de los juegos modernos son, esencialmente, decisiones automatizadas. En el caso de estas decisiones automatizadas, como el bloqueo por fraude, las sanciones por trampas u otras violaciones de los términos y condiciones por parte de los jugadores, o los niveles de emparejamiento, los actores del ecosistema deben establecer en sus especificaciones internas cómo se mantendrá la transparencia de la lógica de umbrales y cómo se comunicarán los canales de revisión humana. Esto es vital para los proveedores de tecnología para el desarrollo, que deben ofrecer soporte a nivel de API para el cumplimiento de derechos y documentar la lógica de los modelos para que los editores puedan proporcionar explicaciones útiles a los jugadores. Por ejemplo, los proveedores que crean las “cuentas de usuario del motor” o los “servicios de perfilado” deben documentar su lógica de manera suficiente para que los editores puedan ofrecer a los jugadores, en diferentes etapas del ciclo de vida, explicaciones sobre por qué se les aplicó una mecánica u oferta específica.

Un sistema conforme al reglamento equilibra la automatización con la supervisión humana. Por ejemplo, la moderación automatizada puede marcar contenido probablemente abusivo, pero las sanciones finales podrían ser confirmadas por un moderador humano o, al menos, estar sujetas a una revisión humana sencilla tras la apelación del interesado. En el caso de las suspensiones automáticas de cuentas (por fraude o violaciones de los términos de servicio), los responsables del tratamiento podrían implementar un botón de “*ticket* de apelación” en el aviso de suspensión con un compromiso de SLA (*Service Level Agreement*) de revisión humana garantizada en 24/48 horas. Los sistemas de emparejamiento pueden utilizar datos personales para determinar los niveles de habilidad de los jugadores, pero si el resultado tiene consecuencias significativas para la progresión o el acceso a recompensas, la lógica del algoritmo debe explicarse en términos comprensibles a petición del interesado. En general, para cualquier moderación o decisión automatizada (por ejemplo, prohibiciones de chat, detección de *exploits*), los responsables del tratamiento deben crear un flujo de trabajo con una plantilla que explique los criterios de decisión (para enviar por correo electrónico o mostrar en la interfaz de usuario), el proceso de apelación y el compromiso de revisión humana.

VI. RECOMENDACIONES Y MEJORES PRÁCTICAS EN LA FASE DE POSPRODUCCIÓN

Una vez que un juego se ha lanzado y ha entrado en su fase de operaciones en vivo a largo plazo, la naturaleza del cumplimiento del RGPD vuelve a cambiar significativamente. Durante la preproducción, la producción y el lanzamiento, el cumplimiento es en gran medida anticipatorio o incipiente: la tarea consiste en diseñar e implementar tratamientos de datos personales lícitos, de conformidad con la ley, y que respeten los derechos y libertades de los interesados. Sin embargo, una vez que el juego está en funcionamiento a largo plazo, el cumplimiento se vuelve completamente operativo. Cada actualización, ciclo de eventos, refactorización del sistema, experimento de monetización o iniciativa de gestión comunitaria conlleva consecuencias en materia de protección de datos. En esta etapa, el reto no consiste tanto en prever o evaluar el riesgo, sino en gestionarlo de manera continua, garantizando que la tecnología en evolución, el comportamiento de la comunidad y las prioridades empresariales no menoscaben los compromisos establecidos durante las primeras etapas del ciclo de vida.

Los juegos son dinámicos. Crecen, se reducen, cambian de forma y de propósito con el tiempo. Algunos títulos operan durante más de una década; otros experimentan una evolución intensa durante los primeros dieciocho meses y luego se estabilizan en ritmos más lentos. Sea cual sea la trayectoria, los responsables siguen siendo responsables del tratamiento de los datos personales hasta el momento en que finaliza el plazo de conservación y la infraestructura del juego se desmantela por completo. Esta responsabilidad se extiende a lo largo de tres períodos operativos principales: las continuas actualizaciones y evolución de funcionalidades, la gobernanza y la seguridad de los datos, y los requisitos legales y éticos que surgen cuando un juego se acerca al final de su vida útil.

A. IDENTIFICACIÓN DE ROLES Y RESPONSABILIDADES EN RELACIÓN CON EL RGPD

La identificación de estos roles debería haberse realizado en la primera etapa del ciclo de vida del juego, pues es una tarea que debe llevarse a cabo durante la preproducción y producción, cuando se planifican todas las actividades de tratamiento de datos personales. Sin embargo, todas las preguntas de orientación relativas al tratamiento que se lleva a cabo una vez que el videojuego está realmente en el mercado se incluyen aquí por claridad. Tal vez algunas preguntas de orientación de las secciones IV.A o V.A también puedan ser útiles a la hora de determinar los roles conforme al RGPD en esta etapa.

VI.A.1 Proveedores de hardware

Preguntas de orientación:

- ¿Mantiene activas las cuentas de la plataforma para volver a captar a jugadores inactivos con eventos, ventas y contenido estacional en muchos juegos? Si es así, responsable del tratamiento de ese uso prolongado de cuentas.
- ¿Cogestiona programas de fidelización a largo plazo con editores (estados compartidos, recompensas entre juegos)? Si es así, evalúe la corresponsabilidad del tratamiento de ese programa.
- ¿Sigue recogiendo y analizando la telemetría de la plataforma (duración de las sesiones, uso del juego, registros de errores) para el ajuste continuo del rendimiento, las

actualizaciones del sistema operativo y la optimización de su *storefront*? Si es así, responsable del tratamiento.

- ¿Los paneles de telemetría a largo plazo para editores se codiseñan, influyendo tanto en sus decisiones como en las de estos (por ejemplo, posicionamiento de contenido, soporte de funcionalidad, actualizaciones)? Si es así, examine la corresponsabilidad del tratamiento de ese servicio de analítica.
- ¿Mantiene perfiles de compromiso a largo plazo en varios juegos para promocionar eventos, suscripciones y lotes de juegos? Si es así, responsable del tratamiento.
- ¿Comparte segmentos ("aficionados al deporte", "grandes gastadores") con editores para campañas que codiseña con ellos? Si es así, considere la corresponsabilidad del tratamiento de esas campañas conjuntas.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuenta de la plataforma de hardware): probablemente responsable del tratamiento, a veces corresponsable del tratamiento o encargado del tratamiento.
- Monitorización del juego (telemetría de plataforma): responsable del tratamiento, corresponsable del tratamiento cuando la telemetría se usa de forma conjunta con editores.
- Inferencia conductual (inferencias de plataforma): probablemente responsable del tratamiento.

VI.A.2 Creadores, diseñadores y desarrolladores

Preguntas de orientación:

- ¿Gestiona las cuentas de su propia comunidad (foros, boletines, programas de recompensas cosméticas) para mantener el compromiso más allá del lanzamiento inicial? Si es así, responsable del tratamiento.
- ¿Gestiona cuentas de jugadores exclusivamente en nombre de un editor (marca del editor, su política de privacidad e instrucciones sobre comunicaciones)? Si es así, encargado del tratamiento para ese tipo de cuentas.
- ¿Sigue operando analítica/monitorización para estabilidad, equilibrio y actualizaciones de contenido estrictamente bajo las instrucciones de un editor? Si es así, sigue siendo encargado del tratamiento para estas actividades y conserve las pruebas de cumplimiento (registros, auditorías).
- ¿Utiliza telemetría a largo plazo en diferentes versiones del juego para informar sobre diseños futuros, curvas de dificultad o modelos de IA? Si es así, responsable del tratamiento de ese uso de I+D/analítica.
- ¿Utiliza historiales de jugadores a largo plazo para crear modelos para nuevos contenidos descargables, pase de temporada o ajustes de monetización en varios títulos? Si es así, responsable del tratamiento de ese perfilado.
- ¿Solo implementa o aloja lógica de perfilado especificada y propiedad del editor, sin reutilización entre clientes? Si es así, encargado del tratamiento para ese flujo de perfilado.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas del juego): responsable del tratamiento para cuentas propias; encargado del tratamiento si las cuentas se gestionan para un editor.
- Monitorización del juego (telemetría del juego): encargado del tratamiento al recoger telemetría exclusivamente para el editor; responsable del tratamiento al usar los datos para I+D propia en diferentes proyectos.
- Inferencia conductual (inferencias del juego): responsable del tratamiento al crear modelos para fines propios; encargado del tratamiento al crear modelos exclusivamente para el editor bajo instrucciones.

VI.A.3 Proveedores de tecnología para el desarrollo

Preguntas de orientación:

- ¿Mantiene activas cuentas de administrador de desarrollador/editor y, posiblemente, cuentas de inicio de sesión único (*Single Sign One* o SSO) para jugadores con fines de analítica a largo plazo, facturación o funcionalidad entre títulos? Si es así, responsable del tratamiento.
- Cuando un cliente utiliza su servicio de gestión de identidad simplemente como un servicio y usted se compromete a no reutilizar los datos más allá de la seguridad técnica ¿actúa bajo sus instrucciones? Si es así, encargado del tratamiento para esa parte.
- ¿Sigue recibiendo telemetría de juegos en directo durante meses/años para mejorar su servicio, el sistema antitrampas o la optimización del motor? Si es así, responsable del tratamiento de ese tratamiento continuo.
- ¿Sigue alojando telemetría exclusivamente para un cliente, bajo sus instrucciones y sin reutilización, tras el lanzamiento? Si es así, las obligaciones como encargado del tratamiento (seguridad, supresión, asistencia) siguen vigentes.
- ¿Sus servicios de optimización de monetización/compromiso están entrenados con datos de muchos títulos y se utilizan como productos genéricos (por ejemplo, un SDK que sugiere el mejor momento para ofertas)? Si es así, responsable del tratamiento de ese perfilado.
- ¿Usted y clientes específicos diseñan de manera conjunta reglas de segmentación y *targeting* en su sistema (por ejemplo, campañas conjuntas)? Si es así, evalúe la corresponsabilidad del tratamiento.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas propias de servicio): responsable del tratamiento; encargado del tratamiento si se limita a autenticar para un cliente.
- Monitorización del juego (telemetría del servicio): a menudo responsable del tratamiento, a veces corresponsable del tratamiento; puede ser encargado del tratamiento si está realmente sujeto a instrucciones.
- Inferencia conductual (inferencias del servicio): responsable del tratamiento para modelos conductuales genéricos (posible corresponsable del tratamiento), a veces encargado del tratamiento.

VI.A.4 Editores

Preguntas de orientación:

- ¿Mantiene activas cuentas del editor para secuelas, contenido descargable, eventos estacionales y marketing entre títulos (correo electrónico, bandeja de entrada en el juego, notificaciones *push*)? Si es así, responsable del tratamiento, con obligaciones continuas.
- ¿Existen programas de fidelización o membresía de marca compartida en los que usted y una plataforma o *storefront* compartan la toma de decisiones sobre ventajas y el uso de datos? Si es así, evalúe la corresponsabilidad del tratamiento de esos programas.
- ¿Ejecuta analítica de operaciones en vivo para monitorizar el compromiso, la adopción de contenido descargable, el abandono y la monetización de forma indefinida o durante muchos años? Si es así, responsable del tratamiento, con responsabilidad a largo plazo en cuanto a la necesidad y la minimización.
- ¿Depende de plataformas de analítica o de marketing de terceros para paneles de control y campañas continuas? Si trabajan estrictamente bajo sus instrucciones, son encargados del tratamiento; si reutilizan datos agregados para su propio negocio, son al menos responsables del tratamiento independientes para esa reutilización.
- ¿Mantiene perfiles detallados (gasto, tiempo de juego, modos, respuesta a ofertas) para ejecutar marketing y personalización dentro del juego continuos durante años? Si es así, responsable del tratamiento.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuentas del editor): responsable del tratamiento; a veces corresponsable del tratamiento con creadores, diseñadores y desarrolladores.
- Monitorización del juego (telemetría del editor): responsable del tratamiento de la telemetría; corresponsable del tratamiento con otros actores cuando deciden conjuntamente.
- Inferencia conductual (inferencias del editor): responsable del tratamiento del perfilado basado en el juego; a veces corresponsable del tratamiento con proveedores de hardware/proveedores de tecnología para el desarrollo/*storefronts*.

VI.A.5 *Storefronts*

Preguntas de orientación:

- ¿Se usan las cuentas del *storefront*/lanzador para gestionar listas de deseos a largo plazo, listas de pendientes, recordatorios y campañas de “vuelve” en diferentes títulos? Si es así, responsable del tratamiento.
- ¿Cogestiona eventos recurrentes (festivales de editores, destacados de franquicias) con listas de membresía compartidas? Si es así, examine la corresponsabilidad del tratamiento de esos programas específicos.
- ¿Utiliza telemetría a largo plazo del *storefront*/lanzador (instalaciones, tiempo de juego, métricas de conversión) para pruebas A/B y estrategias de *merchandising* durante años? Si es así, responsable del tratamiento.
- ¿Algunos programas de analítica se especifican junto con editores (por ejemplo, eventos recurrentes basados en patrones de todo el *storefront*)? Si es así, considere si ese programa en particular implica corresponsabilidad del tratamiento.

- ¿Perfila las compras a largo plazo de los jugadores, el comportamiento en las listas de deseos y el tiempo de juego para seleccionar ventas, eventos y promociones cruzadas? Si es así, responsable del tratamiento de ese perfilado.
- ¿Gestiona programas promocionales conjuntos con editores que dependen de sus perfiles y sus conocimientos (reglas de segmentación compartidas)? Si es así, evalúe la corresponsabilidad del tratamiento de esas campañas.

En resumen, por tipo de actividad de tratamiento de datos:

- Creación y gestión de cuentas (cuenta del *storefront*): responsable del tratamiento; posiblemente corresponsable del tratamiento con editores para programas de marca compartida.
- Monitorización del juego (telemetría del *storefront*): responsable del tratamiento de la telemetría utilizada para gestionar y optimizar el *storefront*/lanzador; corresponsable del tratamiento si codetermina la telemetría con los editores.
- Inferencia conductual (inferencias del *storefront*): responsable del tratamiento de sus propios sistemas de recomendación y publicidad dirigida; a veces corresponsable del tratamiento con editores para campañas conjuntas.

B. GESTIÓN DE OPERACIONES CONTINUAS TRAS EL LANZAMIENTO

VI.B.1 Prevención del desvío de finalidad

Los juegos en funcionamiento no son productos estáticos. Siempre están cambiando: se añade un nuevo sistema de emparejamiento, un evento estacional cambia el comportamiento de los jugadores, un sistema de hermandades se convierte en una plataforma social con más alcance, los equipos de retención solicitan datos más detallados, los diseñadores crean nuevos sistemas de recompensas y los equipos de protección mejoran las herramientas de moderación. Cada cambio puede afectar al tratamiento de los datos personales de los jugadores.

El desvío de finalidad, es decir, la expansión gradual del uso de los datos más allá de su propósito original es un riesgo común en el ecosistema de los videojuegos, donde los datos se acumulan y se generan constantemente y donde los incentivos comerciales están siempre presentes y evolucionan de forma continua. Esto ocurre cuando los datos recogidos para un uso se reutilizan para otro incompatible con la finalidad inicial. Incluso pequeños cambios en la forma en que se interpreta la telemetría o en quién puede acceder a ella pueden alterar la naturaleza y el ámbito del tratamiento con el tiempo. Esto puede dar lugar, en última instancia, a que diferentes actores traten datos para fines no comunicados a los jugadores, incumpliendo el Artículo 5(1)(b) del RGPD.

Este fenómeno es especialmente común cuando crecen las presiones comerciales. Los datos recogidos para depuración pueden convertirse más tarde en un activo atractivo para ofertas personalizadas o precios dinámicos. De manera similar, las señales conductuales recogidas para seguridad pueden parecer útiles para predecir el compromiso o modelar el abandono. El hecho de que estos usos sean tentadores o incluso beneficiosos para las partes interesadas no los hace lícitos. El responsable del tratamiento debe reevaluar si el nuevo uso es compatible con la finalidad original conforme al Artículo 6(4) del reglamento.

El desvío de finalidad también puede ser sutil. Consideremos un juego que recoge indicadores de habilidad para ayudar a realizar emparejamientos justos. Con el tiempo, el

equipo de analítica puede encontrar correlaciones entre las métricas de habilidad y la probabilidad de comprar elementos cosméticos. Si estas métricas se utilizan después para personalizar los *storefronts* o programar promociones, los datos del juego se reutilizan para monetización de una manera que los jugadores no podrían esperar.

Los responsables del tratamiento deben realizar revisiones estructuradas y periódicas de cada actividad de tratamiento de datos para confirmar que el uso de los datos es coherente con la finalidad original. Si no lo es, los responsables del tratamiento deben resolver la discrepancia, ya sea limitando el tratamiento o estableciendo una nueva base jurídica y proporcionando al jugador información actualizada.

Las campañas de actualización del consentimiento también son una buena práctica porque las condiciones originales del consentimiento suelen cambiar sustancialmente, lo que menoscaba el carácter específico e informado del consentimiento si no se revisa. Las expectativas y los contextos de los jugadores también evolucionan (menores que se convierten en adultos, cambios en el estilo de juego, sensibilidad ante el seguimiento, etc.), por lo que la reconfirmación periódica ayuda a preservar la lealtad y la alineación con las expectativas del usuario. Desde una perspectiva de gobernanza, las campañas estructuradas de refresco de consentimiento obligan a los responsables del tratamiento a auditar las finalidades, las bases jurídicas y los registros de consentimiento, a eliminar los consentimientos “huérfanos” o no documentados, y a mejorar los registros, lo que ayuda a evitar el desvío de finalidad y favorece la responsabilidad proactiva.

VI.B.2 Gobierno del ciclo de vida de los datos personales

Los juegos modernos generan conjuntos de datos masivos. Los errores, los fallos, las secuencias de movimiento, las interacciones económicas, los registros de chat, los historiales de progresión y las interacciones sociales se acumulan rápidamente. Si no se controlan, estos conjuntos de datos crecen más allá de lo necesario, proporcionado o seguro. El principio de minimización de datos (Artículo 5(1)(c) del RGPD) exige a los responsables del tratamiento que solo traten lo adecuado, pertinente y necesario. El principio de limitación del plazo de conservación (Artículo 5(1)(e) del RGPD) establece que los datos personales no deben conservarse más tiempo del necesario para los fines del tratamiento.

En la práctica, la minimización de datos no es un compromiso puntual. Es un proceso a largo plazo. Un plan de conservación elaborado al principio del ciclo de vida del juego puede quedarse obsoleto a medida que se añaden o modifican nuevas funcionalidades. Un sistema de chat puede requerir un plazo de conservación más largo para la moderación inicial. Más tarde, cuando se estabilice, los registros a largo plazo pueden dejar de ser necesarios. Un campo de telemetría utilizado durante el mes del lanzamiento para el equilibrio de dificultad puede volverse irrelevante más adelante. Los responsables del tratamiento deben considerar la conservación como un proceso dinámico. Las cuentas inactivas deben archivarse o eliminarse periódicamente, los registros deben eliminarse de forma regular, los campos de telemetría deben evaluarse y retirarse según sea necesario. En general, los archivos deben anonimizarse en la mayor medida posible una vez que hayan finalizado las necesidades operativas de identificación de los interesados.

Además, los diferentes actores que participan en el ecosistema deben garantizar que la minimización se aplique de manera coherente en los entornos de prueba y producción, identificando y eliminando periódicamente los conjuntos de datos que ya no sean necesarios. Los entornos de prueba suelen acumular datos obsoletos, especialmente cuando las versiones evolucionan rápidamente. Estos conjuntos de datos olvidados suelen ser el eslabón más débil en la higiene de datos de un responsable del tratamiento y, si no se gestionan correctamente, pueden convertirse en vectores para las brechas de datos.

La verdadera minimización exige hacer frente a la tendencia cultural, especialmente en los equipos de ingeniería y analítica, de “guardar los datos por si acaso”. Por ello siempre hay que asegurarse de que los datos conservados respalden una finalidad documentada, lícita y explícita conforme al RGPD. Revise y reduzca periódicamente los esquemas de datos eliminando elementos o campos innecesarios; esta práctica respalda directamente el cumplimiento continuo.

Antes de añadir eventos de telemetría o inferencias conductuales a parches o contenido descargable, los creadores, diseñadores y desarrolladores deben: (1) asegurarse de que los responsables del tratamiento estén informados y den su conformidad, y (2) actualizar las políticas pertinentes para reflejar estos cambios. Además, los proveedores de tecnología para el desarrollo deben ofrecer a sus clientes una función de desactivación que pueda utilizarse fácilmente de forma remota con el juego en producción si una auditoría revela un problema legal o de seguridad con su servicio.

VI.B.3 Monitorización continua de flujos de datos y riesgos

El principio de responsabilidad proactiva del RGPD conforme al Artículo 5(2), así como los Artículos 24 y 30, obligan a los responsables del tratamiento a describir y documentar activamente los flujos de datos personales. En concreto, los responsables del tratamiento deben identificar qué equipos acceden a cada conjunto de datos, con qué frecuencia y con qué fines, y mantener esta documentación actualizada para garantizar el cumplimiento.

Los juegos en funcionamiento suelen experimentar cambios estructurales que alteran, aunque sea sutilmente, los flujos de los datos. Al migrar a una nueva región de servidores, introducir un nuevo módulo antitrampas o integrar una herramienta de analítica de terceros, evalúe siempre los impactos en las transferencias internacionales, identifique nuevos encargados del tratamiento y revise las prácticas de conservación. Siempre supervise y documente estos cambios a medida que ocurran.

Las evaluaciones de riesgo y las EIPD no deben reservarse únicamente para reestructuraciones importantes o nuevas funcionalidades. Deben realizarse cuando se produzca cualquier cambio que afecte al flujo de datos, especialmente cuando implique datos de menores o perfilado conductual. También son importantes en el caso de sistemas que puedan tener consecuencias significativas para los jugadores. Las auditorías regulares ayudan a identificar la recogida innecesaria de datos, la conservación excesiva o las finalidades documentadas que han quedado obsoletas.

VI.B.4 Habilitación de la seguridad en un entorno real

Otro principio central del RGPD es el de integridad y confidencialidad (Artículo 5(1)(f) del reglamento). Conforme a este principio, los datos personales deben tratarse de manera que se garanticen niveles adecuados de seguridad frente a, por ejemplo, tratamientos no autorizados o ilícitos. La obligación de los responsables del tratamiento de proteger adecuadamente los datos personales se desarrolla además en el Artículo 32 del RGPD. No puede cumplirse únicamente con el diseño técnico inicial y debe considerarse una obligación continua y permanente.

Los juegos en funcionamiento atraen comportamientos adversarios y amenazas, como la suplantación de cuentas, redes de *bots*, grupos organizados para hacer trampas, fraude con tarjetas de crédito, ataques de *credential stuffing* e intentos de sustraer objetos de alto valor dentro del juego. Por lo tanto, la postura de seguridad de un juego debe evolucionar con el

tiempo para hacer frente a los retos a los que se enfrenta en cada momento. Se recomienda separar las actualizaciones de seguridad importantes que corrigen vulnerabilidades críticas de las actualizaciones funcionales convencionales que añaden nuevas funcionalidades al juego.

Las medidas de seguridad operativa deben incluir: (1) monitorización continua de comportamientos anómalos (tanto de personas como de elementos de código, en particular, elementos externos integrados en el juego); (2) revisiones periódicas de los derechos de acceso (nuevamente, tanto de personas como de elementos de código); (3) escaneo de vulnerabilidades y ejercicios internos de pruebas de penetración o *red teaming*; y (4) auditorías o revisiones periódicas del código. Además, las claves de cifrado deben rotarse cuando se produzcan eventos desencadenantes específicos, la comunicación con los servidores debe protegerse adecuadamente, y la autenticación multifactor debe ser obligatoria tanto para el personal como para cuentas señaladas. Los responsables del tratamiento están obligados a documentar todas estas medidas como parte de sus obligaciones de responsabilidad proactiva.

Cuando se produce una brecha de datos, los Artículos 33 y 34 imponen requisitos estrictos. El responsable del tratamiento debe notificar la brecha a la autoridad de control correspondiente[20] en un plazo de setenta y dos horas desde que tenga conocimiento de esta[21]. Si la brecha entraña un riesgo elevado para los jugadores, el responsable del tratamiento también debe informar directamente a los afectados. La comunicación clara es esencial. Los jugadores deben comprender qué ocurrió, qué datos se vieron comprometidos y qué medidas pueden adoptar. Una brecha nunca debe ser una sorpresa y nunca debe ser descubierta por los jugadores por sus propios medios o a través de los foros de la comunidad. La transparencia es, en este caso, tanto un requisito legal como una obligación ética.

C. PROMOCIÓN DE PRÁCTICAS DE GOBERNANZA MADURAS

VI.C.1 Establecimiento de estructuras y procedimientos

La creciente complejidad de los videojuegos, y en particular de los juegos en línea, exige una gobernanza estructurada en torno al tratamiento de datos personales. Confiar en que los equipos individuales mantengan el cumplimiento de forma independiente suele dar lugar a prácticas fragmentadas y medidas de protección incoherentes. Para cumplir los requisitos establecidos, entre otros, en los Artículos 24 y 25, los responsables del tratamiento deben implementar procesos coordinados. Estos incluyen comités internos de privacidad, auditorías y revisiones multidisciplinares (como revisiones periódicas de decisiones de moderación automatizada) y documentación estandarizada para nuevas actividades de tratamiento.

Además, las comprobaciones de cumplimiento de los encargados y subencargados del tratamiento son esenciales para la gobernanza en el ecosistema de los videojuegos. Los responsables del tratamiento dependen de una cadena de encargados y subencargados del tratamiento (proveedores *cloud*, SDKs publicitarias, empresas de analítica, etc.) para tratar los datos personales. Algunas prácticas recomendadas incluyen auditorías previas a la incorporación de terceros. Estas auditorías revisan las medidas de seguridad de los

[20] EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82022-identifying-controller-or-processors-lead_en

[21] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

encargados del tratamiento, las aportaciones de las EIPD y las listas de subencargados antes de firmar los acuerdos de tratamiento de datos. Otras prácticas se basan en salvaguardas contractuales, como la obligación de incluir derechos de auditoría, procesos de notificación de brechas y la aprobación de subencargados o el "veto del responsable del tratamiento". Las revisiones anuales, incluidas las notificaciones de incidentes, ayudan a mantener los estándares de protección. La alineación con los riesgos específicos de los videojuegos, como evitar patrones de diseño adictivo, también es importante. En general, si un actor que participa en el ecosistema identifica una decisión que afecta a la protección de datos personales, no debe adoptar esa decisión internamente, sino que debe implicar al resto de actores en el proceso de toma de decisiones, teniendo en cuenta sus respectivos roles y obligaciones conforme al RGPD (responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento, subencargado del tratamiento).

Debe tenerse en cuenta que las plantillas compartidas por los actores del ecosistema ayudan a construir el cumplimiento en toda la cadena. Por ejemplo, una plantilla para aprobar cualquier cambio en la implementación de actividades de tratamiento de datos, incluidos los que se producen como parte de una operación de mantenimiento del juego.

Finalmente, las organizaciones deben implementar y fomentar una cultura de refuerzo de la alfabetización en materia de protección de datos y cumplimiento del RGPD mediante formación regular y continua, adaptada a distintos perfiles profesionales. Los desarrolladores y los equipos de operaciones en vivo necesitan formación práctica sobre programación segura y protección de datos desde el diseño, así como sobre los riesgos del perfilado y la toma de decisiones automatizada en los sistemas de emparejamiento, personalización y antitrampas. Los gestores de comunidad, los equipos de marketing y monetización deben recibir módulos de formación específicos sobre las bases jurídicas para la publicidad, el consentimiento y el tratamiento de datos de menores, por ejemplo. Los directivos y los productores deben recibir informes de alto nivel sobre las obligaciones normativas, los desencadenantes de las EIPD y la respuesta ante brechas de datos para que la protección de datos se integre como una expectativa central de gobernanza, no como un aspecto secundario, a lo largo de toda la fase de posproducción.

VI.C.2 Registro de actividades de tratamiento

El Artículo 30 del RGPD obliga a los responsables del tratamiento a mantener registros de las actividades de tratamiento. En el contexto dinámico de los videojuegos, estos registros deben actuar como una herramienta de gobernanza adaptativa, no como un artefacto de cumplimiento estático, y deben actualizarse de manera continua. Cuando se añade un nuevo campo de telemetría, se incorpora un nuevo proveedor, se modifica un plazo de conservación o se retira una funcionalidad, los registros deben revisarse de inmediato. Dada la naturaleza iterativa del desarrollo de juegos, con implementaciones frecuentes de parches, actualizaciones y contenido transitorio, los responsables del tratamiento deben garantizar que todos los cambios que afecten al tratamiento de datos personales se reflejen de inmediato en sus registros.

Los registros exactos y actualizados facilitan el cumplimiento de una serie de obligaciones del RGPD. Permiten a los responsables del tratamiento responder de manera rápida y eficiente a las solicitudes de los interesados, realizar y actualizar las EIPD, gestionar las brechas de datos y defender las decisiones de cumplimiento frente a consultas de las autoridades competentes. Los registros aclaran la responsabilidad interna al documentar las finalidades del tratamiento, las categorías de datos personales, los destinatarios, los plazos de conservación y cualquier transferencia internacional.

Como buena práctica, las empresas del sector de los videojuegos deben integrar el mantenimiento riguroso de registros en los flujos de trabajo de desarrollo y gestión de

productos. De este modo, la documentación permite detectar y mitigar de manera proactiva los riesgos de protección de datos desde fases tempranas hasta la posproducción.

VI.C.3 El papel del delegado de protección de datos

El delegado de protección de datos (DPD), ya sea requerido conforme a los Artículos 37 a 39 del RGPD o nombrado de forma voluntaria, desempeña un papel crítico para garantizar que la protección de datos se considere a lo largo del ciclo de vida de un juego[22]. El DPD debe ser informado de los cambios previstos que puedan afectar al tratamiento de datos personales y debe tener la oportunidad de ofrecer asesoramiento antes de que se adopten decisiones definitivas. Por lo tanto, el DPD debe, entre otras cosas, evaluar nuevas funcionalidades, asesorar sobre las EIPD, supervisar el cumplimiento, auditar las relaciones con los proveedores y evaluar los riesgos, en particular, aquellos relacionados con actividades de alto riesgo, como las prácticas de perfilado o la participación de menores en funcionalidades sociales.

El DPD debe actuar de forma independiente y tener acceso a la alta dirección. Debe poder plantear sus preocupaciones o reservas con libertad. Una organización debe garantizar que su DPD cuente con recursos y apoyo suficientes. El DPD debe recibir la información relevante necesaria para cumplir sus responsabilidades de manera efectiva. Su participación debe ser sustancial e integrada en la gobernanza y la toma de decisiones. No debe limitarse a una consulta formal o a una mera aprobación una vez adoptadas las decisiones clave. Cuando el DPD plantee preocupaciones sobre cambios en el marco del tratamiento de datos personales, esas preocupaciones deben tomarse en serio y documentarse.

D. FIN DE VIDA ÚTIL: RESPONSABILIDADES LEGALES Y TÉCNICAS

Cuando un juego se acerca a su fase final, los responsables del tratamiento afrontan un período de mayor responsabilidad y riesgo que exige una atención rigurosa a medida que el título llega a su fin, independientemente de la causa del cierre. Esta fase de fin de vida útil plantea algunos de los retos más significativos del RGPD, en particular, garantizar la lealtad, la transparencia y la gestión cuidadosa de los datos personales que aún posea el responsable de cada tratamiento.

Conforme a los Artículos 12 a 14 del RGPD, los jugadores deben recibir una notificación clara y, lo antes posible, sobre el cierre del juego. El lenguaje utilizado debe ser inequívoco y debe evitarse ocultar mensajes en materiales de marketing. Los responsables del tratamiento deben describir claramente qué ocurrirá con las cuentas de los jugadores, su progresión, las compras, las comunicaciones y en general, con todos sus datos personales.

Al emitir un aviso de cierre, los responsables del tratamiento deben comunicar la fecha de cierre de los servidores, el plazo para que los jugadores soliciten el acceso o la supresión de sus datos, los tipos de datos que se eliminarán automáticamente y si se conservarán conjuntos de datos anonimizados para investigación y desarrollo. Si se migran jugadores, la migración de cuentas debe tratarse como una actividad de tratamiento independiente y los jugadores deben ser informados.

Una vez finalizado el tratamiento, los datos personales deben suprimirse o anonimizarse de inmediato conforme al Artículo 5(1)(e). Los responsables del tratamiento deben eliminar o anonimizar todos los datos relevantes de los entornos de producción, las copias de seguridad, los sistemas de analítica y los sistemas de los proveedores externos, a menos que estén legalmente obligados a conservarlos. Deben mantener por escrito una política del

[22] WP Article 29 Guidelines on Data Protection Officers ("DPOs"), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_en

ciclo de vida que indique cuándo dejar de comercializar, anonimizar y eliminar los datos en la fase de final de vida del juego.

Al eliminar datos personales, los responsables del tratamiento pueden considerar los siguientes pasos: deshabilitar el acceso al juego; limpiar las bases de datos subyacentes; anonimizar o eliminar los almacenes de datos archivados; enviar instrucciones de supresión a todos los encargados del tratamiento. Deben obtener y guardar confirmación por escrito de cada acción de supresión.

Si se conservan datos para investigación y desarrollo, deben agregar o tratar los datos de telemetría de manera que se impida la reidentificación. Así como verificar que la anonimización cumple los requisitos necesarios y conservar documentación que confirme que la reidentificación no es posible.

ANEXO 1: LISTA DE COMPROBACIÓN PARA PROVEEDORES DE HARDWARE (ESPECIALMENTE FABRICANTES DE CONSOLAS DE VIDEOJUEGOS)

Nota: esta lista de comprobación incluye recomendaciones y buenas prácticas específicas para los videojuegos recogidas en las secciones anteriores de este documento y no tiene por objeto abarcar todas las obligaciones generales o ampliamente conocidas de cumplimiento del RGPD. Debe utilizarse como referencia específica en el sector de los videojuegos y debe complementarse con una revisión jurídica, organizativa y técnica más amplia adecuada a su jurisdicción y a su producto/servicio concreto.

Etapa	Aspecto	Descripción
Preproducción y producción	Responsabilidad proactiva	Enumerar las actividades de tratamiento de datos personales previstas y aplicar el control de roles del RGPD a cada una de ellas
	Responsabilidad proactiva	Documentar la base jurídica y la finalidad (evitando formulaciones genéricas) de cada actividad de tratamiento de datos personales para la que sea responsable del tratamiento
	Responsabilidad proactiva	Elaborar listas de comprobación del proyecto, diccionarios de datos, mapas del ciclo de vida de los datos, etc.
	Responsabilidad proactiva	Clasificar las inferencias y los perfiles conductuales por su impacto potencial para identificar los tratamientos de alto riesgo para los que sea necesaria una EIPD y elaborar secciones específicas de la EIPD relacionadas con estos tratamientos
	Responsabilidad proactiva	Proporcionar los medios y documentación exhaustiva para respaldar el cumplimiento de los demás actores
	DPbDD (Data Protection by Design and by Default)	Definir el esquema mínimo para las cuentas de la plataforma de hardware
	DPbDD	Definir el esquema mínimo para la telemetría de plataforma
	DPbDD	Definir el esquema mínimo para las inferencias de plataforma
	DPbDD	Establecer los plazos de conservación para las cuentas de plataforma de desarrollo/prueba (jugadores de acceso anticipado), la telemetría en bruto, los perfiles conductuales, etc., y diseñar/implementar medidas de cumplimiento, como la purga o supresión automatizadas
	DPbDD	Prohibir por defecto los campos de categorías especiales de datos en los formularios de cuentas, en la telemetría y las inferencias, y

		diseñar/implementar medidas de cumplimiento, como filtros
	DPbDD	Elegir, fomentar y respaldar el tratamiento local de datos
	DPbDD	Diseñar/implementar mecanismos para obtener un consentimiento parental válido de los probadores y jugadores de acceso anticipado menores de edad que lo necesiten
	DPbDD	Ofrecer indicadores de configuración que permitan a los demás actores que participan en el ecosistema desactivar por completo las funciones de perfilado, por ejemplo, en regiones específicas o para cuentas concretas
	DPbDD	Desactivar por defecto los campos de cuentas, la telemetría y las inferencias opcionales o vinculados a la monetización
	DPbDD	Planificar la exclusión voluntaria de la telemetría y las inferencias opcionales o vinculadas a la monetización
	DPbDD	Activar el registro del consentimiento parental para los probadores y jugadores de acceso anticipado menores de edad que lo necesiten
	DPbDD	Diseñar/implementar controles de edad para la adhesión a configuraciones o funcionalidades de riesgo (por ejemplo, garantizar que solo las cuentas marcadas como “adulto” puedan activar el perfilado orientado a la monetización)
	DPbDD	Separar los perfiles de seguridad/funcionales de los perfiles de monetización
	Ejercicio de derechos	Crear *end points* de actualización/exportación/supresión para cuentas de desarrollo/prueba
	Ejercicio de derechos	Etiquetar y documentar las decisiones automatizadas
	Ejercicio de derechos	Diseñar *hooks* de interfaz para la oposición/revisión humana de las decisiones automatizadas
	Seguridad	Exigir la autenticación multifactor para las herramientas de cuentas de desarrollo/prueba
	Seguridad	Utilizar cifrado a nivel de campo en el almacenamiento de perfiles
Lanzamiento	Lealtad y transparencia	Diferenciar claramente entre los datos estrictamente necesarios para el funcionamiento del juego y los datos utilizados para optimizar la monetización

	Lealtad y transparencia	Implementar un centro o sitio de privacidad dedicado
	Lealtad y transparencia	Redactar avisos y políticas de privacidad que citen la base del Artículo 6 para cada actividad de tratamiento de datos personales
	Lealtad y transparencia	Utilizar etiquetas de privacidad o representaciones simplificadas y visuales similares en el momento de la toma de decisiones
	Lealtad y transparencia	Publicar catálogos de telemetría de plataforma, con información sobre eventos, campos, destinatarios y usos
	Consentimiento válido	Garantizar que los mensajes, los menús y las interfaces sean legibles en diferentes dispositivos y entornos
	Consentimiento válido	Bloquear la progresión hasta que se obtenga un consentimiento válido; utilizar avisos por capas
	Consentimiento válido	Presentar las opciones de manera granular y equilibrada, con selectores separados para cada categoría
	Consentimiento válido	Mantener al jugador informado de manera proactiva mediante notificaciones del sistema operativo, notificaciones en la aplicación (ventanas emergentes o *banners*), alertas *push*, advertencias integradas y señales en tiempo real, etc.
	Consentimiento válido	Registrar todas las interacciones relacionadas con el consentimiento (marca de tiempo, ID del dispositivo, opciones seleccionadas) en registros inviolables para garantizar la auditabilidad
	DPbDD	Bloquear/podar el esquema de cuentas de la plataforma
	DPbDD	Bloquear/podar el esquema de telemetría de plataforma
	DPbDD	Bloquear/podar las inferencias de plataforma
	DPbDD	Archivar automáticamente las cuentas de la plataforma inactivas tras un plazo fijo, junto con su telemetría y perfiles asociados (siempre con notificación previa)
	DPbDD	Configurar por defecto la reincorporación de jugadores inactivos con la máxima privacidad
	DPbDD	Analizar los formularios de cuentas, los eventos de telemetría y las inferencias conductuales de plataforma y rechazar las entradas de categorías especiales de datos

	DPbDD	Actualizar los perfiles conductuales de plataforma en periodos de tiempo fijos (limitar las ventanas de perfil) y, cuando sea posible, agregarlos
	DPbDD	Registrar cada caso en que los usuarios o dispositivos se clasifiquen en segmentos conductuales basados en telemetría o inferencias
	DPbDD	Ejecutar *scripts* de verificación para garantizar que las medidas previstas de protección de datos desde el diseño se implementen correctamente
	DPbDD	Implementar mecanismos para la actualización periódica de los modelos de inferencia a nivel de plataforma y para la realización periódica de comprobaciones de sesgo
	Ejercicio de derechos	Ofrecer una interfaz para el ejercicio de derechos integrada en interfaces familiares y nativas del juego para evitar fricciones innecesarias
	Ejercicio de derechos	Crear una página siempre accesible en la que los jugadores puedan ver, editar o rechazar el tratamiento de categorías de datos vinculadas a sus perfiles a nivel de plataforma
	Ejercicio de derechos	Implementar un sistema de *tickets* de soporte al cliente
	Ejercicio de derechos	Responder a las solicitudes de rectificación sin comprometer la integridad del juego ni abrir vías para el abuso
	Ejercicio de derechos	Diseñar mecanismos internos para marcar y aislar los datos para los que el jugador ha solicitado limitar el tratamiento y evitar su uso involuntario en las operaciones en curso
	Ejercicio de derechos	Ofrecer y gestionar un botón de apelación para las suspensiones automatizadas de cuentas a nivel de plataforma (con un SLA para un plazo máximo de revisión)
	Seguridad	Exigir la autenticación multifactor en todos los flujos de recuperación de cuentas de la plataforma
	Seguridad	Utilizar claves únicas y específicas del juego para proteger la transmisión de datos personales desde las consolas hasta los puntos finales en los servidores de *backend*
Posproducción	Responsabilidad proactiva	Realizar revisiones y auditorías estructuradas y periódicas de cada actividad de tratamiento de datos para identificar la recogida innecesaria de

		datos, la conservación excesiva, las finalidades obsoletas, etc.
	Responsabilidad proactiva	Supervisar y documentar los cambios en las actividades de tratamiento de datos a medida que ocurran, garantizando que los responsables del tratamiento estén informados y den su conformidad
	Responsabilidad proactiva	Actualizar regularmente los registros, documentos, avisos, políticas, etc. pertinentes para reflejar estos cambios
	Responsabilidad proactiva	Implementar o participar en procesos coordinados, como comités internos de privacidad, auditorías y revisiones multidisciplinares, documentación estandarizada y plantillas compartidas, etc.
	Responsabilidad proactiva	Realizar comprobaciones periódicas de cumplimiento de los encargados y subencargados del tratamiento
	Responsabilidad proactiva	Exigir a los demás actores del ecosistema, mediante cláusulas contractuales, que notifiquen el final de la vida útil de los juegos y establezcan responsabilidades claras en esta etapa
	Consentimiento válido	Realizar campañas de refresco del consentimiento
	DPbDD	Cesar la recogida de telemetría específica del juego en la fase de final de vida y purgar los datos de telemetría personales almacenados (por ejemplo, estadísticas de uso vinculadas a cuentas); agregar/anonimizar los datos para analítica
	DPbDD	Suprimir o anonimizar las inferencias derivadas del comportamiento en el juego
	Ejercicio de derechos	Informar a los usuarios mediante la consola sobre las opciones en relación con sus datos en la fase de final de vida del juego, permitiéndoles ejercer sus derechos
	Ejercicio de derechos	Apoyar las solicitudes de supresión o anonimización de datos tras el final de vida, ofreciendo a los usuarios procesos claros para solicitar la eliminación de datos personales, como cuentas, telemetría y perfiles vinculados al juego, y conservando únicamente datos anonimizados o legalmente requeridos
	Seguridad	Separar las actualizaciones de seguridad importantes que corrigen vulnerabilidades

		críticas de las actualizaciones funcionales convencionales

ANEXO 2: LISTA DE COMPROBACIÓN PARA CREADORES, DISEÑADORES Y DESARROLLADORES

Nota: esta lista de comprobación incluye recomendaciones y buenas prácticas específicas para los videojuegos recogidas en las secciones anteriores de este documento y no tiene por objeto abarcar todas las obligaciones generales o ampliamente conocidas de cumplimiento del RGPD. Debe utilizarse como referencia específica en el sector de los videojuegos y debe complementarse con una revisión jurídica, organizativa y técnica más amplia adecuada a su jurisdicción y a su producto/servicio concreto.

Etapa	Aspecto	Descripción
Preproducción y producción	Responsabilidad proactiva	Garantizar que los distintos equipos consideran la protección de datos como un requisito de diseño central, equivalente a las consideraciones de juego o narrativa
	Responsabilidad proactiva	Enumerar las actividades de tratamiento de datos personales previstas y aplicar el control de roles del RGPD a cada una de ellas
	Responsabilidad proactiva	Documentar la base jurídica y la finalidad (evitando formulaciones genéricas) de cada actividad de tratamiento de datos personales para la que sea responsable del tratamiento
	Responsabilidad proactiva	Elaborar listas de comprobación del proyecto, diccionarios de datos, mapas del ciclo de vida de los datos, etc.
	Responsabilidad proactiva	Clasificar las inferencias y los perfiles conductuales por su impacto potencial para identificar los tratamientos de alto riesgo para los que sea necesaria una EIPD y elaborar secciones específicas de la EIPD relacionadas con estos tratamientos
	Responsabilidad proactiva	Proporcionar los medios y documentación exhaustiva para respaldar el cumplimiento de los demás actores
	Responsabilidad proactiva	Preparar una plantilla de “aviso de telemetría” para pruebas de juego externas que explique qué se registra durante las pruebas, quién tiene acceso a esos datos y durante cuánto tiempo se registran (esta información debe alinearse con los avisos del editor)
	Responsabilidad proactiva	Añadir una breve “ficha de roles de perfilado” al definir el alcance de las funciones de IA/personalización en preproducción: quién es el propietario, quién puede reutilizarlo y si se actúa como responsable o como encargado del tratamiento

	Responsabilidad proactiva	Divulgar las prácticas de tratamiento de datos de los PNJ mediante avisos contextuales y políticas de privacidad exhaustivas que detallen los flujos, la conservación y la participación de la IA
	DPbDD (Data Protection by Design and by Default)	Definir el esquema mínimo de cuentas del juego
	DPbDD	Definir el esquema mínimo de telemetría del juego
	DPbDD	Etiquetar los eventos de telemetría: “solo para el estudio”, “solo para el editor”, “reutilización por el estudio” (esta última requiere una base jurídica propia y registros de las actividades de tratamiento)
	DPbDD	Definir el esquema mínimo de las inferencias conductuales del juego
	DPbDD	Evaluar los mecanismos y sistemas de progresión del juego para garantizar que no requieran un tratamiento desproporcionado de los datos personales de los jugadores; si existen varias opciones técnicas, seleccionar el diseño menos intrusivo que cumpla los objetivos de juego y narrativa
	DPbDD	Auditar la exactitud del tratamiento de los PNJ impulsados por IA y el sesgo en su toma de decisiones
	DPbDD	Establecer los plazos de conservación para las cuentas de juego de desarrollo/prueba (jugadores de acceso anticipado), la telemetría en bruto, los perfiles conductuales, los datos tratados por los PNJ, etc., y diseñar/implementar medidas de cumplimiento, como la purga o supresión automatizadas
	DPbDD	Prohibir por defecto los campos de categorías especiales de datos en los formularios de cuentas, la telemetría y las inferencias, y diseñar/implementar medidas de cumplimiento, como filtros
	DPbDD	Diseñar la telemetría y las inferencias priorizando el tratamiento local; marcar las cargas servidores externos, por ejemplo, para un permitir un consentimiento granular
	DPbDD	Especificar un umbral de edad al reclutar menores para pruebas de juego anticipadas, crear formularios de consentimiento parental

		separados con registro verificable y garantizar que estos registros se almacenen junto con el ID de cuenta del probador
	DPbDD	Ofrecer indicadores de configuración que permitan a los demás actores que participan en el ecosistema desactivar por completo las funciones de perfilado del juego, por ejemplo, en regiones específicas o para cuentas concretas
	DPbDD	Desactivar por defecto los campos de cuentas, la telemetría y las inferencias opcionales o vinculados a la monetización
	DPbDD	Planificar la exclusión voluntaria de la telemetría y las inferencias del juego opcionales o vinculadas a la monetización
	DPbDD	Integrar la protección de los menores en el diseño y la arquitectura del juego: implementar modos de comunicación restringidos, filtros automatizados, paneles de control para tutores, límites de gasto, restricciones horarias, herramientas de notificación accesibles, etc.
	DPbDD	Diseñar/implementar controles de edad para la adhesión a configuraciones o funcionalidades de riesgo
	DPbDD	Separar los perfiles de seguridad/funcionales de los perfiles de monetización
	DPbDD	Realizar pruebas de UX para detectar patrones engañosos o adictivos mediante auditorías independientes
	DPbDD	Utilizar datos sintéticos, cuando sea posible, para entrenar PNJ impulsados por IA, y minimizar el conjunto de datos de entrenamiento en el resto de los casos mediante la agregación o pseudonimización de las entradas
	Ejercicio de derechos	Crear *end points* de actualización/exportación/supresión para cuentas de desarrollo/prueba
	Ejercicio de derechos	Etiquetar y documentar las decisiones automatizadas
	Ejercicio de derechos	Diseñar *hooks* de interfaz para la oposición/revisión humana de las decisiones automatizadas
	Seguridad	Exigir la autenticación multifactor para las herramientas de cuentas de desarrollo/prueba
	Seguridad	Utilizar cifrado a nivel de campo en el almacenamiento de perfiles

Lanzamiento	Lealtad y transparencia	Diferenciar claramente entre los datos estrictamente necesarios para el funcionamiento del juego y los datos utilizados para optimizar la monetización
	Lealtad y transparencia	Implementar un centro o sitio de privacidad dedicado
	Lealtad y transparencia	Redactar avisos y políticas de privacidad que citen la base del Artículo 6 para cada actividad de tratamiento de datos personales
	Lealtad y transparencia	Utilizar etiquetas de privacidad o representaciones simplificadas y visuales similares en el momento de la toma de decisiones
	Lealtad y transparencia	Publicar catálogos de telemetría del juego, con información sobre eventos, campos, destinatarios y usos
	Lealtad y transparencia	Priorizar los “permisos en tiempo de ejecución” (que se activan cuando se utiliza realmente una función, como el chat de voz) frente a los “permisos en tiempo de instalación”
	Consentimiento válido	Garantizar que los mensajes, los menús y las interfaces sean legibles en diferentes dispositivos y entornos
	Consentimiento válido	Bloquear la progresión hasta que se obtenga un consentimiento válido; utilizar avisos por capas
	Consentimiento válido	Presentar las opciones de manera granular y equilibrada, con selectores separados para cada categoría
	Consentimiento válido	Mantener al jugador informado de manera proactiva mediante notificaciones del sistema operativo, notificaciones en la aplicación (ventanas emergentes o *banners*), alertas *push*, advertencias integradas y señales en tiempo real, etc.
	Consentimiento válido	Registrar todas las interacciones relacionadas con el consentimiento (marca de tiempo, ID del dispositivo, opciones seleccionadas) en registros inviolables para garantizar la auditabilidad
	DPbDD	Bloquear/podar el esquema de cuentas del juego
	DPbDD	Bloquear/podar el esquema de telemetría del juego
	DPbDD	Bloquear/podar las inferencias del juego
	DPbDD	Archivar automáticamente las cuentas del juego inactivas tras un plazo fijo, junto con su

		telemetría y perfiles asociados (siempre con notificación previa)
	DPbDD	Configurar por defecto la reincorporación de jugadores inactivos con la máxima privacidad
	DPbDD	Activar el modo “oculto” por defecto; garantizar que todos los campos opcionales de la cuenta y el intercambio de datos con terceros estén desactivados por defecto, requiriendo una adhesión explícita para su activación
	DPbDD	Analizar los formularios de cuentas, los eventos de telemetría y las inferencias conductuales del juego y rechazar las entradas de categorías especiales de datos
	DPbDD	Actualizar los perfiles conductuales del juego en periodos de tiempo fijos (limitar las ventanas de perfil) y, cuando sea posible, agregarlos
	DPbDD	Registrar cada caso en que los usuarios o dispositivos se clasifiquen en segmentos conductuales basados en telemetría o inferencias
	DPbDD	Ejecutar *scripts* de verificación para garantizar que las medidas previstas de protección de datos desde el diseño se implementen correctamente
	DPbDD	Implementar mecanismos para la actualización periódica de los modelos de inferencia del juego y para la realización periódica de comprobaciones de sesgo
	DPbDD	Fomentar el bienestar de los jugadores incorporando puntos de control, guardados automáticos y pausas naturales (temporizadores de sesión, mensajes de “se sugiere descansar”) para limitar el exceso de participación o compromiso
	Ejercicio de derechos	Ofrecer una interfaz para el ejercicio de derechos integrada en interfaces familiares y nativas del juego para evitar fricciones innecesarias
	Ejercicio de derechos	Crear una página siempre accesible en la que los jugadores puedan ver, editar o rechazar el tratamiento de categorías de datos vinculadas a sus perfiles a nivel de juego
	Ejercicio de derechos	Implementar un sistema de *tickets* de soporte al cliente
	Ejercicio de derechos	Responder a las solicitudes de rectificación sin comprometer la integridad del juego ni abrir vías para el abuso

	Ejercicio de derechos	Diseñar mecanismos internos para marcar y aislar los datos para los que el jugador ha solicitado limitar el tratamiento y evitar su uso involuntario en las operaciones en curso
	Ejercicio de derechos	Ofrecer y gestionar un botón de apelación para las suspensiones automatizadas del juego (con un SLA para un plazo máximo de revisión)
	Seguridad	Exigir la autenticación multifactor en todos los flujos de recuperación de cuentas del juego
	Seguridad	Implementar control de accesos basado en roles para el equipo de desarrollo
	Seguridad	Utilizar claves únicas y específicas del juego para proteger la transmisión de datos personales desde las consolas hasta los puntos finales en los servidores de *backend*
Posproducción	Responsabilidad proactiva	Realizar revisiones y auditorías estructuradas y periódicas de cada actividad de tratamiento de datos para identificar la recogida innecesaria de datos, la conservación excesiva, las finalidades obsoletas, etc.
	Responsabilidad proactiva	Supervisar y documentar los cambios en las actividades de tratamiento de datos a medida que ocurran, garantizando que los responsables del tratamiento estén informados y den su conformidad
	Responsabilidad proactiva	Actualizar regularmente los registros, documentos, avisos, políticas, etc. pertinentes para reflejar estos cambios
	Responsabilidad proactiva	Implementar o participar en procesos coordinados, como comités internos de privacidad, auditorías y revisiones multidisciplinares, documentación estandarizada y plantillas compartidas, etc.
	Responsabilidad proactiva	Realizar comprobaciones periódicas de cumplimiento de los encargados y subencargados del tratamiento
	Responsabilidad proactiva	Notificar el final de la vida útil de los juegos al resto de actores que participan en el ecosistema y establecer responsabilidades claras en esta etapa
	Consentimiento válido	Realizar campañas de refresco del consentimiento
	DPbDD	Garantizar que la minimización se aplique de manera coherente en los entornos de producción y prueba mediante la identificación y eliminación periódicas de los conjuntos de datos que ya no sean necesarios

	DPbDD	Cesar la recogida de telemetría específica del juego en la fase de final de vida y purgar los datos de telemetría personales almacenados (por ejemplo, estadísticas de uso vinculadas a cuentas); agregar/anonimizar los datos para analítica
	DPbDD	Suprimir o anonimizar las inferencias derivadas del comportamiento en el juego
	Ejercicio de derechos	Informar a los usuarios en el propio juego sobre las opciones en relación con sus datos en la fase de final de vida del juego, permitiéndoles ejercer sus derechos
	Ejercicio de derechos	Apoyar las solicitudes de supresión o anonimización de datos tras el final de vida, ofreciendo a los usuarios procesos claros para solicitar la eliminación de datos personales, como cuentas, telemetría y perfiles vinculados al juego, y conservando únicamente datos anonimizados o legalmente requeridos
	Seguridad	Implementar mecanismos de detección de anomalías en las cuentas del juego
	Seguridad	Separar las actualizaciones de seguridad importantes que corrigen vulnerabilidades críticas de las actualizaciones funcionales convencionales

ANEXO 3: LISTA DE COMPROBACIÓN PARA PROVEEDORES DE TECNOLOGÍA PARA EL DESARROLLO

Nota: esta lista de comprobación incluye recomendaciones y buenas prácticas específicas para los videojuegos recogidas en las secciones anteriores de este documento y no tiene por objeto abarcar todas las obligaciones generales o ampliamente conocidas de cumplimiento del RGPD. Debe utilizarse como referencia específica en el sector de los videojuegos y debe complementarse con una revisión jurídica, organizativa y técnica más amplia adecuada a su jurisdicción y a su producto/servicio concreto.

Etapa	**Aspecto**	**Descripción**
Preproducción y producción	Responsabilidad proactiva	Enumerar las actividades de tratamiento de datos personales previstas y aplicar el control de roles del RGPD a cada una de ellas
	Responsabilidad proactiva	Documentar la base jurídica y la finalidad (evitando formulaciones genéricas) de cada actividad de tratamiento de datos personales para la que sea responsable del tratamiento
	Responsabilidad proactiva	Elaborar listas de comprobación del proyecto, diccionarios de datos, mapas del ciclo de vida de los datos, etc.
	Responsabilidad proactiva	Clasificar las inferencias y los perfiles conductuales por su impacto potencial para identificar los tratamientos de alto riesgo para los que sea necesaria una EIPD y elaborar secciones específicas de la EIPD relacionadas con estos tratamientos
	Responsabilidad proactiva	Proporcionar un texto modelo para que los distintos actores que participan en el ecosistema puedan explicar claramente si son corresponsables de la autenticación (por ejemplo: “X autentica tu cuenta en nuestro nombre”)
	Responsabilidad proactiva	Proporcionar los medios y documentación exhaustiva para respaldar el cumplimiento de los demás actores: un diagrama de flujo de datos por producto que enumere explícitamente los campos de datos, los destinatarios, la condición de responsable del tratamiento y las opciones de configuración, cláusulas contractuales tipo, una “ficha de datos de perfilado” detallada para cada módulo conductual (con las entradas, las salidas, las finalidades, el responsable del tratamiento y cómo pueden ejercer sus derechos los interesados), etc.
	Responsabilidad proactiva	Incluir cláusulas contractuales que prohíban a los clientes enviar etiquetas de “menores

		conocidos" a las API de perfilado sin salvaguardas adicionales acordadas
	DPbDD (Data Protection by Design and by Default)	Diseñar el servicio de modo que las funcionalidades (analítica de audiencia, *retargeting* publicitario, etc.) estén desactivadas, permitiendo a los clientes seleccionar solo los módulos que necesiten
	DPbDD	Definir el esquema mínimo para las cuentas del servicio
	DPbDD	Separar las cuentas de "uso de herramientas" (para los equipos de desarrollo) de las cuentas de "jugador"
	DPbDD	Definir el esquema mínimo para la telemetría del servicio
	DPbDD	Definir el esquema mínimo para las inferencias de la SDK
	DPbDD	Establecer los plazos de conservación para las cuentas, la telemetría, los perfiles conductuales del servicio, etc. y diseñar/implementar medidas de cumplimiento, como la purga o supresión automatizada
	DPbDD	Prohibir por defecto los campos de categorías especiales de datos en los formularios de cuentas, en la telemetría y las inferencias, y diseñar/implementar medidas de cumplimiento, como filtros
	DPbDD	Elegir, fomentar y respaldar el tratamiento local de datos
	DPbDD	Ofrecer indicadores de configuración que permitan a los demás actores que participan en el ecosistema desactivar por completo las funciones de perfilado, por ejemplo, en regiones específicas o para cuentas concretas
	DPbDD	Exponer selectores granulares para la sincronización de datos, adhesiones, etc..
	DPbDD	Garantizar que los paneles de control del SDK muestren únicamente métricas agregadas; el acceso a la telemetría en bruto de un jugador debe requerir un proceso de escalado de privilegios limitado en el tiempo y registrado
	DPbDD	Diseñar las herramientas para que acepten y procesen una señal de edad, de modo que las funcionalidades puedan restringirse/activarse automáticamente en función de la edad verificada

	DPbDD	Desactivar por defecto los campos de cuentas, la telemetría y las inferencias opcionales o vinculados a la monetización
	DPbDD	Planificar la exclusión voluntaria de la telemetría y las inferencias opcionales o vinculadas a la monetización
	DPbDD	Separar los perfiles de seguridad/funcionales de los perfiles de monetización
	DPbDD	Realizar pruebas de UX para detectar patrones engañosos o adictivos mediante auditorías independientes
	Ejercicio de derechos	Etiquetar y documentar las decisiones automatizadas
	Ejercicio de derechos	Diseñar *hooks* de interfaz para la oposición/revisión humana de las decisiones automatizadas
	Seguridad	Garantizar la separación lógica, implementando claves o esquemas de base de datos diferentes para cada cliente para evitar accesos *cross-tenant* desde el diseño
	Seguridad	Cifrar las cargas útiles del servicio de extremo a extremo
	Seguridad	Utilizar cifrado a nivel de campo en el almacenamiento de perfiles
Lanzamiento	Lealtad y transparencia	Diferenciar claramente entre los datos estrictamente necesarios para el funcionamiento del servicio y los datos utilizados para optimizar la monetización
	Lealtad y transparencia	Implementar un centro o sitio de privacidad dedicado que incluya un panel de control para transparencia en vivo (por ejemplo, “Perfil utilizado X veces esta semana”)
	Lealtad y transparencia	Redactar avisos y políticas de privacidad que citen la base del Artículo 6 para cada actividad de tratamiento de datos personales
	Lealtad y transparencia	Utilizar etiquetas de privacidad o representaciones simplificadas y visuales similares en el momento de la toma de decisiones
	Lealtad y transparencia	Publicar catálogos de telemetría del SDK, con información sobre eventos, campos, destinatarios y usos
	Consentimiento válido	Garantizar que los mensajes, los menús y las interfaces sean legibles en diferentes dispositivos y entornos

	Consentimiento válido	Presentar las opciones de manera granular y equilibrada, con selectores separados para cada categoría
	Consentimiento válido	Diseñar el servicio para que se pueda suspender su ejecución hasta que la aplicación que lo usa envíe una señal de obtención de consentimiento válido
	Consentimiento válido	Registrar todas las interacciones relacionadas con el consentimiento (marca de tiempo, ID del dispositivo, opciones seleccionadas) en registros inviolables para garantizar la auditabilidad
	DPbDD	Bloquear/podar el esquema de cuentas del servicio
	DPbDD	Bloquear/podar el esquema de telemetría del servicio
	DPbDD	Bloquear/podar las inferencias del servicio
	DPbDD	Archivar automáticamente las cuentas del servicio inactivas tras un plazo fijo, junto con su telemetría y perfiles asociados (siempre con notificación previa)
	DPbDD	Analizar los formularios de cuentas, los eventos de telemetría y las inferencias conductuales del juego y rechazar las entradas de categorías especiales de datos
	DPbDD	Actualizar los perfiles conductuales del SDK en periodos de tiempo fijos (limitar las ventanas de perfil) y, cuando sea posible, agregarlos
	DPbDD	Registrar cada caso en que los usuarios o dispositivos se clasifiquen en segmentos conductuales basados en telemetría o inferencias
	DPbDD	Ejecutar *scripts* de verificación para garantizar que las medidas previstas de protección de datos desde el diseño se implementen correctamente
	DPbDD	Implementar mecanismos para la actualización periódica de los modelos de inferencia del SDK y para la realización periódica de comprobaciones de sesgo
	DPbDD	Desactivar automáticamente las funcionalidades del servicio que no se usan
	Ejercicio de derechos	Ofrecer una interfaz que permita a los clientes reflejar automáticamente las solicitudes de los jugadores (acceso, portabilidad o supresión) en la infraestructura del servicio

	Ejercicio de derechos	Ofrecer una interfaz para el ejercicio de derechos integrada en interfaces familiares y fáciles de usar para evitar fricciones innecesarias
	Ejercicio de derechos	Implementar un sistema de *tickets* de soporte al cliente
	Ejercicio de derechos	Responder a las solicitudes de rectificación sin comprometer la integridad del juego ni abrir vías para el abuso
	Ejercicio de derechos	Diseñar mecanismos internos para marcar y aislar los datos para los que el jugador ha solicitado limitar el tratamiento y evitar su uso involuntario en las operaciones en curso
	Seguridad	Notificar las anomalías a los clientes (por ejemplo, picos inusuales de perfilado)
	Seguridad	Exigir la autenticación multifactor en todos los flujos de recuperación de cuentas del servicio
Posproduccción	Responsabilidad proactiva	Realizar revisiones y auditorías estructuradas y periódicas de cada actividad de tratamiento de datos para identificar la recogida innecesaria de datos, la conservación excesiva, las finalidades obsoletas, etc.
	Responsabilidad proactiva	Supervisar y documentar los cambios en las actividades de tratamiento de datos a medida que ocurran, garantizando que los responsables del tratamiento estén informados y den su conformidad
	Responsabilidad proactiva	Actualizar regularmente los registros, documentos, avisos, políticas, etc. pertinentes para reflejar estos cambios
	Responsabilidad proactiva	Implementar o participar en procesos coordinados, como comités internos de privacidad, auditorías y revisiones multidisciplinares, documentación estandarizada y plantillas compartidas, etc.
	Responsabilidad proactiva	Realizar comprobaciones periódicas de cumplimiento de los encargados y subencargados del tratamiento
	Responsabilidad proactiva	Exigir a los demás actores del ecosistema, mediante cláusulas contractuales, que notifiquen el final de la vida útil de los juegos y establezcan responsabilidades claras en esta etapa
	Consentimiento válido	Garantizar que la revocación del consentimiento de un jugador no provoque

		inestabilidad en el juego ni haga que el servicio solicite permisos de nuevo constantemente
	Consentimiento válido	Realizar campañas de refresco del consentimiento
	DPbDD	Cesar la recogida de telemetría específica del juego en la fase de final de vida y purgar los datos de telemetría personales almacenados (por ejemplo, estadísticas de uso vinculadas a cuentas); agregar/anonimizar los datos para analítica
	DPbDD	Suprimir o anonimizar las inferencias derivadas del comportamiento en el juego
	DPbDD	Actualizar el software periódicamente para aprovechar las últimas API de sistemas operativos y plataformas de hardware que sean más respetuosas con la privacidad
	DPbDD	Ofrecer a los clientes una función de desactivación que pueda utilizarse fácilmente de forma remota en producción si una auditoría revela un problema legal o de seguridad con el software
	Ejercicio de derechos	Apoyar las solicitudes de supresión o anonimización de datos tras el final de vida, ofreciendo a los usuarios procesos claros para solicitar la eliminación de datos personales, como cuentas, telemetría y perfiles vinculados al juego, y conservando únicamente datos anonimizados o legalmente requeridos
	Seguridad	Separar las actualizaciones de seguridad importantes que corrigen vulnerabilidades críticas de las actualizaciones funcionales convencionales

ANEXO 4: LISTA DE COMPROBACIÓN PARA EDITORES

Nota: esta lista de comprobación incluye recomendaciones y buenas prácticas específicas para los videojuegos recogidas en las secciones anteriores de este documento y no tiene por objeto abarcar todas las obligaciones generales o ampliamente conocidas de cumplimiento del RGPD. Debe utilizarse como referencia específica en el sector de los videojuegos y debe complementarse con una revisión jurídica, organizativa y técnica más amplia adecuada a su jurisdicción y a su producto/servicio concreto.

Etapa	Aspecto	Descripción
Preproducción y producción	Responsabilidad proactiva	Enumerar las actividades de tratamiento de datos personales previstas y aplicar el control de roles del RGPD a cada una de ellas
	Responsabilidad proactiva	Documentar la base jurídica y la finalidad (evitando formulaciones genéricas) de cada actividad de tratamiento de datos personales para la que sea responsable del tratamiento
	Responsabilidad proactiva	Elaborar listas de comprobación del proyecto, diccionarios de datos, mapas del ciclo de vida de los datos, etc.
	Responsabilidad proactiva	Clasificar las inferencias y los perfiles conductuales por su impacto potencial para identificar los tratamientos de alto riesgo para los que sea necesaria una EIPD y elaborar secciones específicas de la EIPD relacionadas con estos tratamientos
	Responsabilidad proactiva	Proporcionar los medios y documentación exhaustiva para respaldar el cumplimiento de los demás actores
	Responsabilidad proactiva	Preparar una plantilla de “aviso de telemetría” para pruebas de juego externas que explique qué se registra durante las pruebas, quién tiene acceso a esos datos y durante cuánto tiempo se registran
	Responsabilidad proactiva	Añadir una breve “ficha de roles de perfilado” al definir el alcance de las funciones de IA/personalización en preproducción: quién es el propietario, quién puede reutilizarlo y si se actúa como responsable o como encargado del tratamiento
	DPbDD (Data Protection by Design and by Default)	Definir el esquema mínimo de cuentas del editor. Determinar desde el principio si las cuentas serán por juego o compartidas; en este último caso, limitar los campos de datos por defecto al mínimo común necesario para todos

		los títulos en lugar de a un conjunto de datos amplio
	DPbDD	Mantener una entrada separada para los registros en programas alfa/beta, en la que se reflejen qué datos se recogen (correos electrónicos, edad, ID de plataforma) y si se utilizarán más adelante para marketing o futuros títulos.
	DPbDD	Definir el esquema mínimo de telemetría del editor
	DPbDD	Planificar cómo se vincularán los datos o el perfil del jugador entre varios juegos y hacer que esta vinculación sea opcional
	DPbDD	Etiquetar los eventos de telemetría: “solo para el estudio”, “solo para el editor”, “reutilización por el estudio”
	DPbDD	Definir el esquema mínimo de las inferencias conductuales del editor
	DPbDD	Establecer los plazos de conservación para las cuentas del editor, la telemetría en bruto, los perfiles conductuales, etc., y diseñar/implementar medidas de cumplimiento, como la purga o supresión automatizadas
	DPbDD	Prohibir por defecto los campos de categorías especiales de datos en los formularios de cuentas, la telemetría y las inferencias, y diseñar/implementar medidas de cumplimiento, como filtros
	DPbDD	Utilizar por defecto datos de prueba sintéticos o fuertemente anonimizados; evitar los datos reales de jugadores en entornos de desarrollo y preproducción
	DPbDD	Diseñar la telemetría y las inferencias priorizando el tratamiento local; marcar las cargas servidores externos, por ejemplo, para un permitir un consentimiento granular
	DPbDD	Especificar un umbral de edad al reclutar menores para pruebas de juego anticipadas, crear formularios de consentimiento parental separados con registro verificable y garantizar que estos registros se almacenen junto con el ID de cuenta del probador
	DPbDD	Si el editor ofrece servicios diferentes, permitir que el jugador utilice cada uno de los servicios de forma independiente

	DPbDD	Desactivar por defecto los campos de cuentas, la telemetría y las inferencias opcionales o vinculados a la monetización
	DPbDD	Planificar la exclusión voluntaria de la telemetría y las inferencias del editor opcionales o vinculadas a la monetización
	DPbDD	Diseñar/implementar controles de edad para la adhesión a configuraciones o funcionalidades de riesgo
	DPbDD	Separar los perfiles de seguridad/funcionales de los perfiles de monetización
	DPbDD	Realizar pruebas de UX para detectar patrones engañosos o adictivos mediante auditorías independientes e incentivar de manera explícita a los creadores, diseñadores y desarrolladores para no utilizar este tipo de patrones
	DPbDD	Minimizar los datos transmitidos a socios comerciales y proveedores externos, enviando datos identificativos (nombre, alias o apodo, número de identificador único, etc.) solo cuando sea estrictamente necesario
	Ejercicio de derechos	Crear *end points* de actualización/exportación/supresión para cuentas de desarrollo/prueba
	Ejercicio de derechos	Especificar en los acuerdos alfa/beta con los probadores si la telemetría está anonimizada/agregada y si se utilizará para futuros títulos o perfilado, ajustando los mecanismos de transparencia y elección en consecuencia
	Ejercicio de derechos	Etiquetar y documentar las decisiones automatizadas
	Ejercicio de derechos	Diseñar *hooks* de interfaz para la oposición/revisión humana de las decisiones automatizadas
	Seguridad	Proteger las cuentas con almacenamiento seguro de contraseñas, MFA cuando proceda (por ejemplo, para usuarios administrativos), protección de sesiones, limitación de frecuencia de peticiones y detección de abusos
	Seguridad	Utilizar cifrado a nivel de campo en el almacenamiento de perfiles
Lanzamiento	Lealtad y transparencia	Diferenciar claramente entre los datos estrictamente necesarios para el funcionamiento del juego y los datos utilizados para optimizar la monetización

	Lealtad y transparencia	Informar a los jugadores sobre la transmisión de sus datos personales a socios comerciales y proveedores externos
	Lealtad y transparencia	Implementar un centro o sitio de privacidad dedicado
	Lealtad y transparencia	Redactar avisos y políticas de privacidad que citen la base del Artículo 6 para cada actividad de tratamiento de datos personales
	Lealtad y transparencia	Utilizar etiquetas de privacidad o representaciones simplificadas y visuales similares en el momento de la toma de decisiones
	Lealtad y transparencia	Publicar catálogos de telemetría del editor, con información sobre eventos, campos, destinatarios y usos
	Consentimiento válido	Garantizar que los mensajes, los menús y las interfaces sean legibles en diferentes dispositivos y entornos
	Consentimiento válido	Presentar las opciones de manera granular y equilibrada, con selectores separados para cada categoría y evitando el consentimiento por lotes (por ejemplo, asegurar que el consentimiento para marketing es independiente de la aceptación de los Términos y condiciones del servicio)
	Consentimiento válido	Registrar todas las interacciones relacionadas con el consentimiento (marca de tiempo, ID del dispositivo, opciones seleccionadas) en registros inviolables para garantizar la auditabilidad
	DPbDD	Bloquear/podar el esquema de cuentas del editor
	DPbDD	Bloquear/podar el esquema de telemetría del editor
	DPbDD	Bloquear/podar las inferencias del editor
	DPbDD	Archivar automáticamente las cuentas del editor inactivas tras un plazo fijo, junto con su telemetría y perfiles asociados (siempre con notificación previa)
	DPbDD	Activar el modo “oculto” por defecto; garantizar que todos los campos opcionales de la cuenta y el intercambio de datos con terceros estén desactivados por defecto, requiriendo una adhesión explícita para su activación
	DPbDD	Analizar los formularios de cuentas, los eventos de telemetría y las inferencias conductuales del

		editor y rechazar las entradas de categorías especiales de datos
	DPbDD	Actualizar los perfiles conductuales del editor en periodos de tiempo fijos (limitar las ventanas de perfil) y, cuando sea posible, agregarlos
	DPbDD	Registrar cada caso en que los usuarios o dispositivos se clasifiquen en segmentos conductuales basados en telemetría o inferencias
	DPbDD	Ejecutar *scripts* de verificación para garantizar que las medidas previstas de protección de datos desde el diseño se implementen correctamente
	DPbDD	Implementar mecanismos para la actualización periódica de los modelos de inferencia del editor y para la realización periódica de comprobaciones de sesgo
	Ejercicio de derechos	Ofrecer una interfaz para el ejercicio de derechos integrada en interfaces familiares y nativas del juego para evitar fricciones innecesarias y proporcionar una herramienta única para acceder, rectificar o suprimir datos personales en diferentes títulos
	Ejercicio de derechos	Crear una página siempre accesible en la que los jugadores puedan ver, editar o rechazar el tratamiento de categorías de datos vinculadas a sus perfiles a nivel de editor
	Ejercicio de derechos	Identificar los datos portables y facilitar las exportaciones mediante coordinación respaldada por contratos (garantizar que las tiendas o los desarrolladores propaguen las solicitudes en todo el ecosistema, etc.)
	Ejercicio de derechos	Implementar una función central de exclusión voluntaria que bloquee la telemetría o las inferencias conductuales en todos los títulos, con opciones de exclusión que persistan tras las reinstalaciones
	Ejercicio de derechos	Implementar un sistema de *tickets* de soporte al cliente
	Ejercicio de derechos	Diseñar mecanismos internos para marcar y aislar los datos para los que el jugador ha solicitado limitar el tratamiento y evitar su uso involuntario en las operaciones en curso
	Ejercicio de derechos	Ofrecer a los jugadores explicaciones sobre por qué han sido objeto de una mecánica u oferta específica

	Ejercicio de derechos	Diseñar una herramienta centralizada e interna que permita hacer un seguimiento y gestionar todas las sanciones dentro del juego (prohibiciones, suspensiones, etc.) y las apelaciones asociadas de los jugadores en todo el catálogo de títulos (no solo por juego)
	Seguridad	Separar claramente los sistemas de bases de datos (o, al menos, sus esquemas y los controles de acceso) para los datos principales del juego/servicio (cuentas, progreso, pagos, emparejamiento, etc.) y los datos de marketing/CRM/analítica (listas de correo, seguimiento de campañas, datos de atribución, etc.)
Posproducción	Responsabilidad proactiva	Realizar revisiones y auditorías estructuradas y periódicas de cada actividad de tratamiento de datos para identificar la recogida innecesaria de datos, la conservación excesiva, las finalidades obsoletas, etc.
	Responsabilidad proactiva	Establecer un proceso de validación para aprobar cualquier cambio en las condiciones de implementación de los tratamientos de datos personales, incluidas las modificaciones que se produzcan como parte de una operación de mantenimiento del juego
	Responsabilidad proactiva	Supervisar y documentar los cambios en las actividades de tratamiento de datos a medida que ocurran, garantizando que los responsables del tratamiento estén informados y den su conformidad
	Responsabilidad proactiva	Actualizar regularmente los registros, documentos, avisos, políticas, etc. pertinentes para reflejar estos cambios
	Responsabilidad proactiva	Implementar o participar en procesos coordinados, como comités internos de privacidad, auditorías y revisiones multidisciplinares, documentación estandarizada y plantillas compartidas, etc.
	Responsabilidad proactiva	Realizar comprobaciones periódicas de cumplimiento de los encargados y subencargados del tratamiento
	Consentimiento válido	Realizar campañas de refresco del consentimiento
	DPbDD	Reevaluar si todos los flujos de telemetría y las inferencias siguen siendo necesarios tras el lanzamiento, y eliminar aquellos que ya no cumplan una finalidad documentada

	DPbDD	Cesar la recogida de telemetría específica del juego en la fase de final de vida y purgar los datos de telemetría personales almacenados (por ejemplo, estadísticas de uso vinculadas a cuentas); agregar/anonimizar los datos para analítica
	DPbDD	Suprimir o anonimizar las inferencias derivadas del comportamiento en el juego
	Ejercicio de derechos	Informar a los usuarios en el propio juego sobre las opciones en relación con sus datos en la fase de final de vida del juego, permitiéndoles ejercer sus derechos
	Ejercicio de derechos	Apoyar las solicitudes de supresión o anonimización de datos tras el final de vida, ofreciendo a los usuarios procesos claros para solicitar la eliminación de datos personales, como cuentas, telemetría y perfiles vinculados al juego, y conservando únicamente datos anonimizados o legalmente requeridos
	Seguridad	Implementar mecanismos de detección de anomalías en las cuentas del editor
	Seguridad	Mantener manuales de respuesta ante incidentes para el compromiso de cuentas, brechas de datos de telemetría e inferencias o exposición accidental de los sistemas de prueba

ANEXO 5: LISTA DE COMPROBACIÓN PARA *STOREFRONTS*

Nota: esta lista de comprobación incluye recomendaciones y buenas prácticas específicas para los videojuegos recogidas en las secciones anteriores de este documento y no tiene por objeto abarcar todas las obligaciones generales o ampliamente conocidas de cumplimiento del RGPD. Debe utilizarse como referencia específica en el sector de los videojuegos y debe complementarse con una revisión jurídica, organizativa y técnica más amplia adecuada a su jurisdicción y a su producto/servicio concreto.

Etapa	**Aspecto**	**Descripción**
Preproducción y producción	Responsabilidad proactiva	Enumerar las actividades de tratamiento de datos personales previstas y aplicar el control de roles del RGPD a cada una de ellas
	Responsabilidad proactiva	Documentar la base jurídica y la finalidad (evitando formulaciones genéricas) de cada actividad de tratamiento de datos personales para la que sea responsable del tratamiento
	Responsabilidad proactiva	Elaborar listas de comprobación del proyecto, diccionarios de datos, mapas del ciclo de vida de los datos, etc.
	Responsabilidad proactiva	Clasificar las inferencias y los perfiles conductuales por su impacto potencial para identificar los tratamientos de alto riesgo para los que sea necesaria una EIPD y elaborar secciones específicas de la EIPD relacionadas con estos tratamientos
	Responsabilidad proactiva	Proporcionar los medios y documentación exhaustiva para respaldar el cumplimiento de los demás actores (por ejemplo, un “documento resumen de roles” para cada programa alfa/beta dirigido a los editores, para que ambas partes puedan alinear sus avisos de privacidad o las EIPD)
	Responsabilidad proactiva	Al configurar programas alfa/beta a través de la tienda, aclarar en los contratos qué consentimientos/avisos muestra la tienda, qué datos recibe el editor y bajo qué rol (responsable independiente o encargado del tratamiento)
	Responsabilidad proactiva	Preparar una plantilla de “aviso de telemetría” para pruebas externas que explique qué se registra durante las pruebas, quién tiene acceso a esos datos y durante cuánto tiempo se registran
	Responsabilidad proactiva	Añadir una breve “ficha de roles de perfilado” al definir el alcance de las funciones de

		IA/personalización en preproducción: quién es el propietario, quién puede reutilizarlo y si se actúa como responsable o como encargado del tratamiento
	DPbDD (Data Protection by Design and by Default)	Definir el esquema mínimo de cuentas del *storefront*. Determinar desde el principio si las cuentas serán por juego o compartidas; en este último caso, limitar los campos de datos por defecto al mínimo común necesario para todos los títulos en lugar de a un conjunto de datos amplio
	DPbDD	Mantener una entrada separada para los registros en programas alfa/beta, en la que se reflejen qué datos se recogen (correos electrónicos, edad, ID de plataforma) y si se utilizarán más adelante para marketing o futuros títulos
	DPbDD	Definir el esquema mínimo de telemetría del *storefront*
	DPbDD	Planificar cómo se vincularán los datos o el perfil del jugador entre varios juegos y hacer que esta vinculación sea opcional
	DPbDD	Etiquetar los eventos de telemetría (“editor”, “*storefront*”, etc.) y distinguir claramente la analítica de la tienda de la analítica por juego
	DPbDD	Definir el esquema mínimo de las inferencias conductuales del *storefront*
	DPbDD	Establecer los plazos de conservación para las cuentas del *storefront*, la telemetría en bruto, los perfiles conductuales, etc., y diseñar/implementar medidas de cumplimiento, como la purga o supresión automatizadas
	DPbDD	Prohibir por defecto los campos de categorías especiales de datos en los formularios de cuentas, la telemetría y las inferencias, y diseñar/implementar medidas de cumplimiento, como filtros
	DPbDD	Utilizar por defecto datos de prueba sintéticos o fuertemente anonimizados; evitar los datos reales de jugadores en entornos de desarrollo y preproducción
	DPbDD	Diseñar la telemetría y las inferencias priorizando el tratamiento local; marcar las cargas servidores externos, por ejemplo, para un permitir un consentimiento granular
	DPbDD	Especificar un umbral de edad al reclutar menores para pruebas de juego anticipadas,

		crear formularios de consentimiento parental separados con registro verificable y garantizar que estos registros se almacenen junto con el ID de cuenta del probador
	DPbDD	Desactivar por defecto los campos de cuentas, la telemetría y las inferencias opcionales o vinculados a la monetización
	DPbDD	Planificar la exclusión voluntaria de la telemetría y las inferencias del *storefront* opcionales o vinculadas a la monetización
	DPbDD	Diseñar/implementar controles de edad para la adhesión a configuraciones o funcionalidades de riesgo
	DPbDD	Separar los perfiles de seguridad/funcionales de los perfiles de monetización
	DPbDD	Realizar pruebas de UX para detectar patrones engañosos o adictivos mediante auditorías independientes e incentivar de manera explícita a los creadores, diseñadores y desarrolladores para no utilizar este tipo de patrones
	DPbDD	Minimizar los datos transmitidos a socios comerciales y proveedores externos, enviando datos identificativos (nombre, alias o apodo, número de identificador único, etc.) solo cuando sea estrictamente necesario
	Ejercicio de derechos	Crear *end points* de actualización/exportación/supresión para cuentas de desarrollo/prueba
	Ejercicio de derechos	Especificar en los acuerdos alfa/beta con los probadores si la telemetría está anonimizada/agregada y si se utilizará para futuros títulos o perfilado, ajustando los mecanismos de transparencia y elección en consecuencia
	Ejercicio de derechos	Etiquetar y documentar las decisiones automatizadas
	Ejercicio de derechos	Diseñar *hooks* de interfaz para la oposición/revisión humana de las decisiones automatizadas
	Seguridad	Proteger las cuentas con almacenamiento seguro de contraseñas, MFA cuando proceda (por ejemplo, para usuarios administrativos), protección de sesiones, limitación de frecuencia de peticiones y detección de abusos
	Seguridad	Utilizar cifrado a nivel de campo en el almacenamiento de perfiles

Lanzamiento	Lealtad y transparencia	Garantizar que toda la información relacionada con la privacidad y las clasificaciones por edades PEGI estén disponibles para el usuario antes de que se haga clic en el botón de compra o descarga
	Lealtad y transparencia	Diferenciar claramente entre los datos estrictamente necesarios para el funcionamiento del juego y los datos utilizados para optimizar la monetización
	Lealtad y transparencia	Ofrecer filtros de privacidad en las opciones de búsqueda para que los jugadores puedan encontrar juegos con/sin prácticas específicas de tratamiento de datos
	Lealtad y transparencia	Informar a los jugadores sobre la transmisión de sus datos personales a socios comerciales y proveedores externos
	Lealtad y transparencia	Implementar un centro o sitio de privacidad dedicado
	Lealtad y transparencia	Redactar avisos y políticas de privacidad que citen la base del Artículo 6 para cada actividad de tratamiento de datos personales
	Lealtad y transparencia	Utilizar etiquetas de privacidad o representaciones simplificadas y visuales similares en el momento de la toma de decisiones
	Lealtad y transparencia	Publicar catálogos de telemetría del *storefront*, con información sobre eventos, campos, destinatarios y usos
	Lealtad y transparencia	Ofrecer herramientas de denuncia dentro del lanzador para que los jugadores puedan señalar diferentes amenazas, como contenido dañino, o diseños engañosos o adictivos en los juegos
	Consentimiento válido	Garantizar que los mensajes, los menús y las interfaces sean legibles en diferentes dispositivos y entornos
	Consentimiento válido	Presentar las opciones de manera granular y equilibrada, con selectores separados para cada categoría y evitando el consentimiento por lotes (por ejemplo, asegurar que el consentimiento para marketing es independiente de la aceptación de los Términos y condiciones del servicio)
	Consentimiento válido	Registrar todas las interacciones relacionadas con el consentimiento (marca de tiempo, ID del dispositivo, opciones seleccionadas) en

		registros inviolables para garantizar la auditabilidad
	DPbDD	Bloquear/podar el esquema de cuentas del *storefront*
	DPbDD	Bloquear/podar el esquema de telemetría del *storefront*
	DPbDD	Bloquear/podar las inferencias del *storefront*
	DPbDD	Archivar automáticamente las cuentas del *storefront* inactivas tras un plazo fijo, junto con su telemetría y perfiles asociados (siempre con notificación previa)
	DPbDD	Activar el modo “oculto” por defecto; garantizar que todos los campos opcionales de la cuenta y el intercambio de datos con terceros estén desactivados por defecto, requiriendo una adhesión explícita para su activación
	DPbDD	Analizar los formularios de cuentas, los eventos de telemetría y las inferencias conductuales del *storefront* y rechazar las entradas de categorías especiales de datos
	DPbDD	Actualizar los perfiles conductuales del *storefront* en periodos de tiempo fijos (limitar las ventanas de perfil) y, cuando sea posible, agregarlos
	DPbDD	Registrar cada caso en que los usuarios o dispositivos se clasifiquen en segmentos conductuales basados en telemetría o inferencias
	DPbDD	Ejecutar *scripts* de verificación para garantizar que las medidas previstas de protección de datos desde el diseño se implementen correctamente
	DPbDD	Implementar mecanismos para la actualización periódica de los modelos de inferencia del *storefront* y para la realización periódica de comprobaciones de sesgo
	Ejercicio de derechos	Ofrecer una interfaz para el ejercicio de derechos integrada en interfaces familiares y nativas del juego para evitar fricciones innecesarias y proporcionar una herramienta única para acceder, rectificar o suprimir datos personales en diferentes títulos
	Ejercicio de derechos	Crear una página siempre accesible en la que los jugadores puedan ver, editar o rechazar el tratamiento de categorías de datos vinculadas a sus perfiles a nivel de *storefront*

	Ejercicio de derechos	Identificar los datos portables y facilitar las exportaciones mediante coordinación respaldada por contratos
	Ejercicio de derechos	Implementar una función central de exclusión voluntaria que bloquee la telemetría o las inferencias conductuales en todos los títulos, con opciones de exclusión que persistan tras las reinstalaciones
	Ejercicio de derechos	Implementar un sistema de *tickets* de soporte al cliente
	Ejercicio de derechos	Diseñar mecanismos internos para marcar y aislar los datos para los que el jugador ha solicitado limitar el tratamiento y evitar su uso involuntario en las operaciones en curso
	Ejercicio de derechos	Ofrecer a los jugadores explicaciones sobre por qué han sido objeto de una oferta específica
	Ejercicio de derechos	Diseñar una herramienta centralizada e interna que permita hacer un seguimiento y gestionar todas las sanciones dentro del juego (prohibiciones, suspensiones, etc.) y las apelaciones asociadas de los jugadores en todo el catálogo de títulos (no solo por juego)
	Seguridad	Separar claramente los sistemas de bases de datos (o, al menos, sus esquemas y los controles de acceso) para los datos principales del juego/servicio (cuentas, progreso, pagos, emparejamiento, etc.) y los datos de marketing/CRM/analítica (listas de correo, seguimiento de campañas, datos de atribución, etc.)
Posproducción	Responsabilidad proactiva	Realizar revisiones y auditorías estructuradas y periódicas de cada actividad de tratamiento de datos para identificar la recogida innecesaria de datos, la conservación excesiva, las finalidades obsoletas, etc.
	Responsabilidad proactiva	Establecer un proceso de validación para aprobar cualquier cambio en las condiciones de implementación de los tratamientos de datos personales, incluidas las modificaciones que se produzcan como parte de una operación de mantenimiento del juego
	Responsabilidad proactiva	Supervisar y documentar los cambios en las actividades de tratamiento de datos a medida que ocurran, garantizando que los responsables del tratamiento estén informados y den su conformidad

	Responsabilidad proactiva	Actualizar regularmente los registros, documentos, avisos, políticas, etc. pertinentes para reflejar estos cambios
	Responsabilidad proactiva	Implementar o participar en procesos coordinados, como comités internos de privacidad, auditorías y revisiones multidisciplinares, documentación estandarizada y plantillas compartidas, etc.
	Responsabilidad proactiva	Realizar comprobaciones periódicas de cumplimiento de los encargados y subencargados del tratamiento
	Consentimiento válido	Realizar campañas de refresco del consentimiento
	DPbDD	Reevaluar si todos los flujos de telemetría y las inferencias siguen siendo necesarios tras el lanzamiento, y eliminar aquellos que ya no cumplan una finalidad documentada
	DPbDD	Cesar la recogida de telemetría específica del juego en la fase de final de vida y purgar los datos de telemetría personales almacenados (por ejemplo, estadísticas de uso vinculadas a cuentas); agregar/anonimizar los datos para analítica
	DPbDD	Suprimir o anonimizar las inferencias derivadas del comportamiento en el juego
	Ejercicio de derechos	Informar a los usuarios en el propio juego sobre las opciones en relación con sus datos en la fase de final de vida del juego, permitiéndoles ejercer sus derechos
	Ejercicio de derechos	Apoyar las solicitudes de supresión o anonimización de datos tras el final de vida, ofreciendo a los usuarios procesos claros para solicitar la eliminación de datos personales, como cuentas, telemetría y perfiles vinculados al juego, y conservando únicamente datos anonimizados o legalmente requeridos
	Seguridad	Implementar mecanismos de detección de anomalías en las cuentas del *storefront*
	Seguridad	Mantener manuales de respuesta ante incidentes para el compromiso de cuentas, brechas de datos de telemetría e inferencias o exposición accidental de los sistemas de prueba