Premio de Investigación en Protección de Datos Personales Emilio Aced 2020

Protección de datos en el sector de los videojuegos: análisis de su adaptación al RGPD y LOPDgdd desde el punto de vista de los videojuegos de gran presupuesto o «triple A».

Autor: Darío López Rincón

15 de noviembre de 2020

Índice

Glosario y abreviaturas

Abreviaturas utilizadas

RGPD	Reglamento General de Protección de Datos.
LOPDgdd	Ley Orgánica de Protección de Datos y garantía de los derechos digitales.
LSSICE	Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
Reglamento e-privacy	Reglamento Europeo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas.
Privacy Shield	Decisión de ejecución 2016/1250 sobre la adecuación de la protección conferida por el escudo de la privacidad UE-EE. UU.
Schrems II	Resolución C-311/18 Data Protection Commissioner /Maximillian Schrems y Facebook Ireland.
COPPA	Children's Online Privacy Protection Act.
EDPB	Comité Europeo de Protección de Datos en sus siglas en inglés.
EDPS	Supervisor Europeo de Protección de Datos en sus siglas en inglés.
AEPD	Agencia Española de Protección de Datos.
APDCAT	Autoridad Catalana de Protección de Datos.
ICO	Autoridad británica de Protección de Datos por sus siglas en inglés.
CNIL	Autoridad francesa de protección de datos por sus siglas en francés.
DPO/DPD	Delegado de protección de datos.
EEE	Espacio Económico Europeo.
TJUE	Tribunal de Justicia de la Unión Europea.

Terminología sectorial utilizada

Indie	Proyecto que cuenta con un pequeño presupuesto para ser desarrollado, generalmente, el capital que los propios desarrolladores pueden reunir personalmente o través de campañas de crowdfunding.
Publisher	Concepto que coloquialmente engloba a la editora y a la distribuidora de un videojuego, sin perjuicio, de puedan ser dos entidades totalmente distintas.

Estudio	Equipo de profesionales, ya sean desarrolladores, programadores, escritores diseñadores de niveles, diseñadores gráficos, animadores o cualquier otro perfil necesario, que en conjunto crean el videojuego, generalmente conformados como Sociedad.
Crossplay	Funcionalidad que permite a jugadores de distintas plataformas separada, entrar en una misma partida.
Launcher	Aplicación o programa que sirve de pasarela de juego obligatoria para gran parte de los videojuegos en la actualidad.
ID, nickname o batle tag	Seudónimo o apodo que cada jugador decide utilizar de manera pública en el videojuego.
eSports	Competición profesionalizada individual o por equipos organizada sobre un determinado videojuego concreto. El diccionario de la RAE no reconoce expresamente este anglicismo, y recomienda su traducción al castellano como «*deportes electrónicos*».
Triple A	Denominación utilizada para referirse a aquellos videojuegos que cuenta con un gran presupuesto, y que, generalmente, son los que el gran público conoce como videojuegos.
Game as a Service	Modelo de negocio tendente a transformar el videojuego de un producto de pago único a otro que permita ingresos periódicos a través de la generación continua de contenido.
EULA	End User License Agreement.
Loot boxes o cajas de botín	Conjuntos de objetos digitales obtenidos de manera aleatoria a cambio de un precio.
ESRB	Entertainment Software Rating Board.
AEVI	Asociación Española de Videojuegos.
DEV	Asociación Española de Empresas Productoras y Desarrolladoras de Videojuegos y Software de Entretenimiento.
ISFE	Interactive Software Federation Of Europe.
EGDF	European Games Developer Federation.
PEGI	Sistema de etiquetado de videojuegos a nivel europeo.
Micropagos	Compras dentro del videojuego.
Skins	Elementos cosméticos que permiten variar la apariencia del personaje u otros parámetros, generalmente, a cambio de un micropago.
First party	Estudio de desarrollo propiedad del publisher. También se aplica esta denominación a los videojuegos que crean dichos estudios no independientes.

1. Introducción y planteamiento general del estudio

El sector de los videojuegos, conocido habitualmente por el nombre de «industria de los videojuegos», es uno de los ámbitos económicos mundiales más lucrativos del mundo, con una facturación estimada a nivel global de 159.000 millones de dólares[1]. Pasándolo a clave nacional, España se conforma como el noveno mercado mundial con una facturación de 2.583 millones de euros[2] y con 15 millones de jugadores activos, aproximadamente[3].

Unido a esto, es un sector basado completamente en la tecnología desde sus inicios[4], en el que cada vez se obtienen más datos para poder ajustar mejor el videojuego y comprender cómo se comporta el jugador, espoleado por el uso hegemónico del Big Data, y con un grado de automatización casi total para poder gestionar adecuadamente el servicio prestado. Asimismo, cuenta con una presencia bastante importante de menores de edad, en principio, solo en todos aquellos juegos con una calificación de edad que lo permita.

Expresado en términos de privacidad, supone que es un campo en el que se da un tratamiento habitual y muy intenso de datos personales, en algunos casos de manera totalmente automatizada, que afectaría a menores en un porcentaje importante, y que por el número de jugadores habituales que existen en España, afectaría a una parte significativa de la población (*aproximadamente un 32% de la población*). A pesar de su gran popularidad como una de las principales opciones de ocio, todavía es una frontera en la que la protección de datos no tiene un papel tan protagónico como debería en atención a un tratamiento de datos personales tan intenso.

1.1. Objeto y alcance del estudio

El objeto del presente estudio es analizar el estado de cumplimiento en materia de protección de datos y privacidad del sector de los videojuegos con incidencia en España y sus ciudadanos, especialmente en aquellos tratamientos más intensos e invasivos de los que no tiene verdadera constancia el jugador, así como proponer medidas enfocadas en legitimar aquellos elementos o tratamientos que pudieran considerarse legítimos.

El análisis se centrará en el ámbito de los denominados videojuegos «triple A» o de gran presupuesto de corte multijugador configurados como «Game as a service[5]» y las entidades que están detrás de los mismos, por ser los que reúnen un tratamiento de datos personales más intensivo y son las que realmente afectan a los interesados/jugadores españoles, en su gran mayoría.

---

[1] Cifras publicadas por la consultora especializada en analítica en el sector de los videojuegos y los eSports, entre otros, en su último informe del año 2020: «Newzoo Global Games Market Report 2020».

[2] Datos publicados por la Asociación Española de Empresas Productoras y Desarrolladoras de Videojuegos y Software de Entretenimiento (conocida coloquialmente como DEV) en su último libro blanco o análisis anual del sector en 2019: «libro blanco del desarrollo español de videojuegos 2019».

[3] Datos publicados por la Asociación Española de Distribuidores y Editores de Software de Entretenimiento, conocido actualmente como Asociación Española de Videojuegos (AEVI), en su último anuario del año 2019: «La industria del videojuego en España – Anuario 2019».

[4] La innovación en hardware y software es una constante de este sector, representado de manera reconocible para el gran público por las distintas generaciones de consolas que salen al mercado periódicamente. Sin olvidar todas las mejores continuas en distintas tecnologías para conseguir un mejor rendimiento, un apartado gráfico, o una mayor inmersión del jugador.

[5] Con dicha denominación, se pretende hacer referencia a aquellos videojuegos creados por grandes multinacionales con el objetivo de sacar al mercado un título que puede generar ingresos durante un largo período de tiempo, generalmente a través de compras dentro del juego de elementos estéticos, modificadores para avanzar más rápido, o de colecciones de objetos digitales aleatorios, denominados coloquialmente como «loot boxes» (*modelos freemium, free to play, con micropagos, o pay to win*). Como ejemplos más conocidos a nivel general, cabe destacar Fornite: Battle Royale, League of Legends, o Candy Crush.

Este enfoque se plantea como el único que permite realizar un verdadero análisis y estudio del sector, debido a que fuera de estos casos de grandes videojuegos comercializados en múltiples países con multinacionales detrás, no existiría un cumplimiento efectivo de protección de datos que pudiera sustentar un análisis y estudio real, más allá de poner de manifiesto la ausencia del mismo. Asimismo, parte de esos actores que están dentro del alcance de este estudio son las empresas que en la mayoría de casos adquieren los derechos de explotación del videojuego para comercializado y distribuirlo (*publishing*), exigiendo en ese proceso la adopción de sus propios textos legales y estructura.

Desde el punto de vista subjetivo, se pone el foco en el jugador como interesado en esta materia, y afectado aquellos tratamientos específicos del sector que se llevan a cabo. En el análisis se hablará del juego a través de plataforma digital, también conocida como «launcher», debido a que en la actualidad no solo es la vía hegemónica para hacerlo, sino que prácticamente ninguno juego moderno se ejecuta fuera de este sistema[6]

Intentando aportar la mayor practicidad posible, y por ser algo que no aportaría un valor real, se sustituyen las tablas o esquemas por capturas de ejemplos reales de los distintos elementos que se van a exponer con el único objetivo de ilustrar la situación actual de distintos apartados de privacidad en el sector de los videojuegos, y sin tener en ningún momento intención de que sirva como señalamiento del incumplimiento de ninguna de las entidades a las que pertenecieran dichas capturas. Para garantizar este último punta, se procederá a anonimizar cualquier referencia o logotipo a las entidades que pertenezcan dichas capturas.

En atención a la materia tratada, el término «interesado» se sustituirá por el de «jugado*r*» por ser el concepto más adecuado para referirse al afectado por el tratamiento de sus datos personales en un videojuego.

1.2. Metodología y fuentes utilizadas

Para la consecución de los objetivos declarados, el planteamiento de este estudio se basa en tres puntos entrelazados, que toman como hilo conductor y estructura principal los puntos del RGPD en su orden literal:

- Análisis pormenorizado de las cláusulas informativas, políticas de privacidad, dashboards, ejercicio de derechos, así como cualquier otro elemento de privacidad al que al autor tiene acceso como usuario de las plataformas de juegos de las entidades objeto de estudio, con el objetivo de extraer el estado general y promedio del determinado elemento de privacidad a valorar en cada apartado.
- Valoración jurídica de la adecuación de cada uno de esos elementos en atención al tenor literal de la normativa de protección (*RGPD y LOPDgdd*), así como a la interpretación objetiva que las distintas autoridades de protección de datos han dado sobre cuestiones que no quedan debidamente aclaradas en el propio texto normativo, en forma de las directrices, informe y guías publicadas.
- Propuesta de soluciones para aquellos elementos analizados que se considera que no cumplen adecuadamente, dejando fuera aquellos que solamente implicarán mejorar o completar ciertos elementos menores para lograr un cumplimiento efectivo en materia de protección de datos.

[6] Cada vez existen más plataformas propietarias que centralizan los juegos del mismo titular. Como ejemplos ilustrativos tenemos: Battle.net con sus éxitos como World of Warcraft, los fabricantes de consolas con sus versiones exclusivas para sus plataformas, como Microsoft – Xbox o Sony-Playstation; o los grandes vendedores digitales que actúan como plataformas de juego como Steam, o Epic Games Store con su éxito mundial Fornite.

En relación a las fuentes utilizadas para el presente estudio, se referenciarán todos los documentos legales, de autoridades y normativos utilizados en el apartado de bibliografía, junto con un enlace para poder consultarlos en el caso de ser posible. Asimismo, desde el siguiente enlace (materiales) podrá accederse a un repositorio en nube con todos los documentos utilizados, sin necesidad de ulteriores búsquedas o recopilación. En materia de videojuegos existe cierta bibliografía, tanto en lengua española como inglesa, desde el punto de vista de la propiedad intelectual o enfocado a garantizar la protección en el medio digital de los menores, pero no en la materia objeto de este estudio[7].

[7] Existen múltiples publicaciones cortas en formato de pequeño ensayo o valoración en diversos medios y blogs, pero ninguno de ellos entra a analizar las peculiaridades del sector desde la óptica de protección de datos, más allá de exponer que el sector de los videojuegos debe cumplir con el RGPD al igual que el resto de sectores en los que se traten datos personales, o plantear algún punto de manera muy liviana.

2- Estudio

2. Análisis del sector siguiendo el orden marco por el RGPD

Desde la efectiva aplicación del Reglamento General de Protección de Datos (*RGPD*), el pasado 25 de mayo de 2018, los grandes actores de este sector han puesto en marcha un proceso de adaptación en la materia para todos aquellos jugadores de la Unión Europea, Noruega, Liechtenstein e Islandia[8], pero que a pesar de que a primera vista cumpliría de manera muy cualificada, no reuniría ciertos elementos exigidos por la normativa, especialmente en lo que a información y transparencia se refiere en aquellos tratamientos totalmente automatizados.

2.1. Datos tratados en el sector de los videojuegos

Antes de entrar en el análisis del sector de los videojuegos siguiendo el orden marcado por el RGPD, cabe indicar, de manera ejemplificativa, los principales tipos de datos personales que se tratan para dar una idea general e introductoria de la dimensión del estudio y del tratamiento de datos personales en los videojuegos.

2.1.1. Datos recopilados del jugador

Todos aquellos datos que el propio jugador suministra directa y conscientemente. En particular los siguientes:

- Los datos identificativos y de contacto como nombre y apellidos[9], correo electrónico, nickname o «nombre de jugador», dirección física en caso de adquisición de juegos o contenido digital (*a efectos de facturación*), número de teléfono (*como parte del proceso de compra, o como elemento de seguridad para el famoso doble control de seguridad contraseña y sms*), datos de usuario de otras cuentas con las que el jugador se haya autenticado (*se juega en una plataforma y se utiliza ese mismo usuario y contraseña para crear un perfil en otra por comodidad, o para acceder a alguna recompensa o funcionalidad adicional en el juego[10]*). Generalmente, la plataforma de destino es la del editor del videojuego o publisher, del que se hablará en el apartado relativo a los responsables, corresponsables y encargados de tratamiento en este sector
- Características personales: fecha de nacimiento, edad, género, nacionalidad o idioma.
- Datos de facturación y económicos: tarjetas con las que se procede al pago, historial de pedidos y reembolsos.
- Datos de categoría especial: en principio, no se recogerían este tipo de datos por ninguna vía ni se inferirían de los jugadores en general, pero puede existir en relación a los jugadores profesionales en torneos organizados (*eSports*) por la propia compañía, como, por ejemplo, información sobre intolerancias o alergias para el catering interno de eventos concretos.

[8] Al igual que otras muchas normas europeas, el RGPD despliega sus efectos jurídicos en el territorio conformado por estos países y la organización internacional de integración, que es la propia Unión Europa.

[9] En algunos casos se habilita la posibilidad de que el nombre y apellidos sean conocidos por el resto de jugadores considerados como amigos en la plataforma, aunque esto implica eliminar una de las medidas de confidencialidad por defecto que se aplica en el sector, como es el nombre de usuario o nickname *(seudónimo*).

[10] Es usual que se incentive esta autenticación con la cuenta de una tercera plataforma a través de la indicación al jugador de que es una forma más rápida de acceso que la tradicional, y, por tanto, que tardaría menos en entrar para jugar.

2.1.2. Datos observados del jugador

Todos aquellos obtenidos de la monitorización del jugador. En particular los siguientes:

- Datos de actividad y juego: registros de actividad y de partida, fecha y hora, país, región, historial de restricciones de la cuenta, sanciones activas, información de casos, historial de quejas, o registros de chats y otras herramientas de comunicación, entre otros. En algunos casos, también ciertos datos de jugadores profesionales al organizar un torneo concreto: estadísticas o equipo al que pertenecen. Todo ellos a través de cookies y tecnologías equivalentes.
- IP y datos de dispositivo: IP de cada dispositivo desde el que se acceda a la plataforma, historial de navegación, historial de sesiones, modelo y marca del mismo, sistema operativo, navegador, hardware y software (*para comprobar mediante un escaneo de algún programa o archivo malicioso o que permita abusos y trampas en el juego*)
- Otros datos: metadatos y datos mixtos obtenidos de múltiples tratamientos y gestión de información.

2.1.3. Datos inferidos del jugador

Los relativos a la elaboración de distintos perfiles, conclusiones y decisiones, automatizadas y totalmente automatizadas: generación de estadísticas de juegos y concesión de logros, preferencias del jugador para elaborar un perfil, historial de partidas, mensajes publicados en chats dentro de partidas o fuera de ellas.

2.1.4. Datos anónimos y mixtos en los videojuegos

Los videojuegos al igual que en otros sectores con un fuerte componente digital, gestionan una cantidad inconmensurable de todo tipo de datos, siendo muy complicado por el propio funcionamiento del sector y de la capacidad técnica (*propia o contratada*) de los actores objeto de estudio, hablar de verdaderos datos anónimos que no permitan por sí mismos o en conexión con otros identificar a una persona sin aplicar esfuerzos desproporcionados[11].

Todos esos datos que un principio pudieran considerarse como datos anónimos (*firmware instalado en la consola o dispositivo, versiones de juegos instalados, drivers instalados, configuración de pantalla, calidad de la conexión, tiempo de carga*), realmente deberían ser considerados datos mixtos porque se recopilan, monitorizan y se asocian al perfil de jugador u otro identificador utilizado por el responsable para crear un conjunto de datos que poder analizar y valorar periódicamente o en tiempo real, si ese jugador vulnera de algún modo la seguridad del sistema o los servidores, o, por ejemplo, afecta negativamente al resto de jugadores[12]

Sería discutible que ese conjunto de datos posteriormente pudiera disociarse en datos personales o no personales retirando elementos identificativos, por ejemplo la IP o identificador de usuario, ya que con toda esa información específica y en tiempo real cabría la posibilidad de que el jugador fuera reidentificado o que el sistema pueda

[11] Como recuerda la Agencia Federal Alemana en su «Documento de posición para la anonimización bajo el RGPD con especial consideración del sector de las telecomunicaciones», de 29 de junio de 2020, la anonimización que no permita de modo alguno reidentificar a la persona es prácticamente imposible, por lo que la pauta relevante sería que solo pueda volver a asociarse con la persona con un gasto desproporcionado de tiempo, costes o trabajo.

[12] Además del mantenimiento de la seguridad y disponibilidad en los videojuegos como en cualquier otro servicio digital, en este sector se debe aplicar un control adicional de los jugadores para prevenir cualquier acto, generalmente técnico, que altere el equilibro en partida y afecte a la experiencia de juego del resto de participantes.

inferirlo[13],reconstruirlo[14] o volverlo a asociar para detectar a un jugador que encaje en esos parámetros técnicos, aun cuando se hubiera abierto una cuenta nueva para intentar eludir la identificación y cualquier sistema antitrampas o sanción aplicada.

Como marca el Reglamento Europeo de Datos no personales[15], y recuerda la Comisión Europea en sus orientaciones sobre el mismo[16], en el caso de que no pueda desligarse ambos tipos de datos, y aunque los datos personales sean una pequeña parte del total, se aplicará el RGPD a todo el conjunto.

Finalmente cabe destacar, que se utilizan con frecuencia técnicas de anonimización sobre los datos de cada perfil de jugador para generar infografías o estadísticas sobre el funcionamiento o ciertos hitos del videojuego que se quieran destacar públicamente, como, por ejemplo, el número de horas de juego total, logros totales conseguidos, porcentaje de jugadores que han escogido una u otra opción, o personaje jugable más utilizado, entre otras.

2.2. Bases de legitimación

De las 6 bases de legitimación disponibles, dejando fuera del análisis al interés público y el interés vital por no ser posibles, en la industria se utilizan de manera casi exclusiva el consentimiento, la ejecución del contrato y el interés legítimo, junto con una muy puntual referencia a la obligación legal. En este apartado se va a proceder a exponer la

situación de estas cuatro bases de legitimación restante, los usos en el sector, el análisis jurídico de los mismo, y ejemplos reales de los supuestos comentados.

2.2.1 El consentimiento en los videojuegos

En el sector de los videojuegos, y como en gran parte del ámbito de la sociedad de la información, se hace un uso intensivo de esta base bajo la premisa de que, si el interesado lo autoriza, el tratamiento es más garantista y otorga un mayor control al interesado[17]. Se propone esta base en relación con aquellos tratamiento más invasivos y específicos, como el control del jugador por el sistema anti trampas, los sistemas totalmente automatizados para castigar conductas contrarias a los términos y condiciones, o diversos procesos de profiling que se analizarán en el apartado específico[18].

Podrían distinguirse tres momentos distintos en los que se solicita el consentimiento al jugador:

---

[13] Tres criterios de valoración utilizados generalmente para medir si la anonimización es tal: individualización, correlación e inferencia.

[14] En materia de cookies, o más concretamente en técnicas de fingerprinting y Cookie syncing, es posible reconstruir y volver a identificar al usuario que haya borrado la determinada cookie, a través del identificador que se asignó en un principio, y que se envió fuera del dispositivo a un tercero.

[15] Reglamento (UE) 2018/1807, relativo a un marco para la libre circulación de datos no personales en la
Unión Europea, de 14 de noviembre de 2018.

[16] Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, de 9 mayo de 2019.

[17] El EDPB en sus directrices 5/2020 recuerda que el consentimiento que es una base de legitimación más, que deberá valorarse en cada caso si es la más adecuada– puntos 2 y 3, pág 5.

[18] Cabría matizar que el perfilado totalmente automatizado generado con técnicas de Big Data del usuario, no se justifica generalmente por esta vía del consentimiento, sino que se enuncia el uso del interés legítimo, a pesar de podría no ser la más adecuada, sin tener en cuenta los requisitos adicionales que el artículo 22 del RGPD exigiría.

- En el momento de configuración inicial del videojuego o creación del perfil del jugador necesario. Es en este punto concreto en el que se le muestra al jugador toda la documentación legal y consentimientos, generando un intento de «*consentimiento ómnibus*» que abarque con la pulsación de un único botón la aceptación de la licencia y términos y condiciones, política de privacidad, cookies, y licencias otorgadas por terceros para elementos técnicos necesarios para que funcione el videojuego[19].
- En momentos posteriores, y no en todos los casos, para consentir aquellos tratamiento más invasivos y específicos, mencionados con anterioridad, o las modificaciones realizadas en los propios textos legales.
- Consentimiento con motivo del envío de comunicaciones comerciales y de interés. En este apartado no procede realizar un comentario en profundidad, debido a que generalmente se cumplen con las pautas necesarias: no se envía ningún tipo de información hasta que efectivamente se ha marcado la casilla, en cada uno de los envíos se incluye un sistema de oposición al envío de la misma, e incluso en algunos casos, se habilita un dashboard específicos en la cuenta de jugador para marcar y desmarcar los distintos tipos de comunicaciones comerciales existentes. Elemento distinto es el de las cookies y diversa publicidad comportamental que puede aparecer en varios espacios designados o como pop-up, que se analizará en el apartado específico de cookies y otras tecnologías equivalentes.

Siguiendo lo marcado en el artículo 6.1.a y 7 del RGPD, los considerandos 32, 42 y 43 y las directrices 5/2020 del EDPB[20], cabe analizar si el consentimiento en el sector de los videojuegos cumple con los requisitos exigibles para esta figura, y, por tanto, actúa un consentimiento real y efectivo.

i) Manifestación libre de voluntad

Siguiendo la doctrina de unificar toda la información legal en una única pantalla con múltiples enlaces a los distintos textos, de manera casi hegemónica, se habilita una única casilla de aceptación (*y log para demostrar que el jugador ha aceptado*), tanto para los términos y condiciones del videojuego (*End User License Agreement o E.U.L.A en su acepción en inglés*), como para el resto de textos legales. Asimismo, este consentimiento legal único es la única forma de avanzar en la configuración previa del juego.

Este escenario conlleva un riesgo de inducir a confusión en el jugador sobre la mera aceptación de los términos y condiciones de la licencia de uso doméstica y no exclusiva que se le otorga al jugador[21], y del consentimiento en materia de protección de datos que se pide. Particularmente, podría justificarse que no cumple el requisito de ser verdaderamente libre, en atención a cuatro motivos principales[22]:

- Existe un desequilibro claro entre el jugador y el responsable al tratarse de condiciones impuestas al jugador, que, por la mera naturaleza de las mismas, deberían derivarse hacia la base de la ejecución del contrato.

[19] Por ejemplo, los conocidos complementos específicos del ámbito multimedia: Directx o Microsoft Visual C++ de Microsoft, sobre los que se ha construido la determinada versión del videojuego a la que se quiera acceder, y que son necesario para ejecutarla correctamente.
[20] Actualizadas en el año 2020 con la numeración 5/2020: «Guidelines 05/2020 on consent under Regulation 2016/679», de 4 de mayo.
[21] Elemento que el EDPB advierte en sus directrices 2/2019 sobre ejecución del contrato como elemento a tener muy en cuenta para que el responsable del tratamiento no confunda aceptación de un contrato con consentimiento en datos personales en su punto 20, pág 8.
[22] Considerando 43 del RGPD.

- Es condicional por exigirlo como parte no negociable del proceso de configuración del juego, y en su caso, de la creación del perfil del jugador.
- No existe una granularidad suficiente por esa configuración única en bloque de aceptación, y no permite autorizar por separado los distintos tratamientos que existen. Salvando las distancias, sería equiparable a un «*cookie wall*» considerado ilegal en materia de cookies.
- Retirarlo sin perjuicio: no existe una verdadera posibilidad de retirar el consentimiento prestado porque se confunden en uno único lo siguiente: la aceptación de la licencia que nada tiene que ver con protección de datos, el presunto consentimiento para la aceptación de los tratamientos de protección de datos (*a través de la equívoca figura de «acepto la política de privacidad»*), y el propio consentimiento relativo a las cookies.

ii) Específico

En relación con el consentimiento inicial que se exige para poder finalizar ese proceso de configuración y poder jugar no podría determinarse que existe una verdadera especificidad que permita al jugador tener un control sobre los datos, ni determinar a qué fines de tratamiento distintos se está otorgando el consentimiento, ya que, en la propia política de privacidad, y a pesar de ese consentimiento ómnibus de «acepto la política de privacidad» mencionado, se concretan solo varios de los tratamientos llevados a cabo. Además del hecho de no informarse con concreción en una 1º capa en el momento de obtención del consentimiento.

Asimismo, sería complicado justificar que ese consentimiento único se ha planteado así porque agrupa una o varias actividades o tratamientos con un mismo fin[23], ya que en ningún momento se mencionan finalidades concretas y legítimas para las que se autoriza el tratamiento, ni conformaría en realidad un único grupo.

En este planteamiento, podría darse una desviación de uso (*o function creep[24]*) de los datos personales para otros propósitos distintos, debido a que la única información disponible es la de la política de privacidad global en la que se mezclan tratamientos por distintas vías (*o en alguno caso, ejemplos de tratamientos con distintas bases*) que se llevan a cabo. Lo anterior siempre que el jugador pinche sobre el enlace que le redirige a la misma para informarse.

En relación con el otro consentimiento que se configura para esos otros tratamientos más técnicos, y para cambios en las políticas de privacidad, aplicaría el mismo análisis realizado. Se solicita el consentimiento junto con un enlace al texto de la política, pero sin informar realmente de manera adecuada y específica, o si existe algún cambio en las finalidades previamente aceptadas.

iii) Informado

En relación con este punto, no se aprecia la existencia de toda la información que el artículo 13 del RGPD exige como mínima, ni se especifica la posibilidad de retirar dicho consentimiento por una vía igual de fácil y accesible por la que fue otorgarlo.

Además, como recuerda el EDPB en las ya mencionadas directrices sobre el consentimiento[25], podría ser necesario dar más información que la estrictamente marcado por el RGPD, en atención a que el interesado entienda realmente los

[23] Considerando 32 del RGPD.

[24] Uno de los principales riesgos por incumplir el requisito de especificación del consentimiento, enunciado por el EDPB en sus directrices 5/2020 sobre el consentimiento, el ICO en su guía general sobre el RGPD: «Guide to the General Data Protection Regulation (GDPR)», o como escenario de riesgo en las metodologías de análisis de riesgos y evaluaciones de impacto.

[25]Elemento referenciado en el punto 65 de las directrices 5/2020 sobre consentimiento, 3º frase, pág 16.

parámetros del tratamiento en casos especiales o complejos, y cumplir, por tanto, con el fin del derecho de información de que el interesado realmente comprenda el tratamiento planteado. Este punto se analizará en el apartado dedicado a transparencia e información.

Cabe apuntar que la mera referencia a un párrafo genérico dentro de los términos y condiciones, como suele ser el caso general de este sector, sería contrario a la dispuesto específicamente por el EDPB a este respecto[26].

iv) Inequívoco o clara acción afirmativa

Aunque la redacción del texto de la casilla de consentimiento cumple con el requisito de ser afirmativa y con una estructura clara, no puede entenderse como inequívoco porque no implica una aceptación de un tratamiento concreto y que no lleve a error al jugador al no saber a qué ha prestado realmente consentimiento. A pesar de lo anterior, la modalidad de obtención del consentimiento a través de una casilla de opt-in sería adecuada, con la salvedad de que deberían configurarse varias en atención a aquellos tratamientos distintos sobre el consentimiento.

v) Demostrable

Este punto es imposible valorar su cumplimiento ya que no existe posibilidad de acceso a los elementos de prueba necesarios, en particular, al registro de los distintos logs de consentimientos prestados con fecha y hora exacta, así como una copia de la información suministrada en ese momento. En la documentación suministrada en el ejercicio de derecho de acceso no se referencia, y tras la apertura de la cuenta de jugador, únicamente recibe en su correo un mensaje de bienvenida general sin ninguna mención a privacidad u otro aspecto legal.

vi) Revocable

Recordando lo dispuesto en el RGPD y matizado por el EDPB, el interesado debe poder retirar su consentimiento en cualquier momento y de una manera tan fácil como fue darlo, es decir, que, si el consentimiento se obtiene por un clic del ratón, deslizando el dedo o pulsando un botón, debe retirarse siguiendo la misma pauta.

Aplicado al caso de estudio, el consentimiento no es revocable en esos términos, ya que en el caso de que se permita, no es posible realizado desde la propia interfaz del videojuego o su launcher (*a efectos, la app dentro de la que se ejecutarían todos los videojuegos de un mismo publisher*), sino desde el perfil de jugador externo, generalmente, tras múltiples pantallas que no dejan claro esta posibilidad[27].

vii) Posición del Tribunal Constitucional sobre el consentimiento en el ámbito digital

La Sala 2º del Tribunal Constitucional en su Resolución de 27/2020, de 24 de febrero sobre el conocido caso de la publicación en un medio de la imagen obtenida en redes sociales de una víctima, además de dictar resolución sobre este punto, establece una serie de valoraciones pertinentes sobre el propio consentimiento que se dan en el ámbito digital, y que pueden aplicarse al objeto de estudio:

- El ámbito digital no cambia las reglas del juego: que el interesado comparta voluntariamente contenido, no debe entenderse automáticamente como un

[26] Punto 71 de las directrices 5/2020 sobre el consentimiento, 3º frase, pág 17.

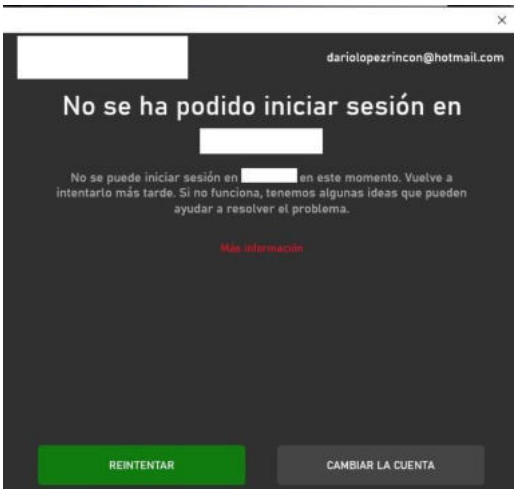
[27] El propio EDPB en el punto 114 de las directrices 5/2020 sobre consentimiento determina esta exigencia de que el consentimiento dado en el marco de una interfaz de usuario de una web, app o cuenta, debe poder retirarse por esa misma vía, sin que pueda justificarse el cambiar a otra interfaz distinta.

consentimiento válido para ser observado, o para que ese contenido se publique o utilice por terceros. En definitiva, se estaría excediendo las legítimas expectativas del titular al subir ese contenido, o en el caso de estudio, para legitimar tratamientos de los que no se ha informado suficientemente.

- Condiciones generales insuficientes y no válidas si no se cumplen los requisitos del consentimiento y el deber de información plenamente, es decir, dar una información: clara, sucinta y completa. Asimismo, la activación por defecto como contenido público no debería estar activada ab initio[28].
- Control del usuario: ha de prevalecer el deber de garantizar el control de la información publicada, junto con la dotación de herramientas para ejercer los derechos que corresponda de manera automática, sencilla, rápida y gratuita.
- Los metadatos han de tenerse en cuenta como datos personales si permiten conocer elementos que identifican a la persona, como, por ejemplo, la autoría.

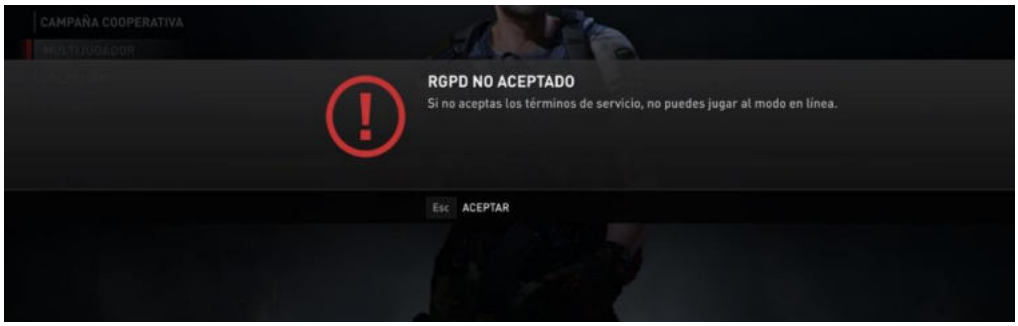
viii) Ejemplos reales de los elementos comentados sobre el consentimiento

Ejemplos de 1º capas informativas y de consentimiento «ómnibus» en el proceso de configuración previo a poder jugar (*izquierda*); y de consentimiento que obliga a aceptar la cesión de datos al «videojuego», sin aclarar si se referencia al publisher titular de los derechos, al estudio desarrollador, o a ambos (*derecha*).



[28] En la mayoría de casos se encuentran activadas por defecto (*también se incluye generalmente deslizadores dentro del perfil de jugador para desactivarlos*), mostrando información al resto de jugadores sobre los logros que has conseguido por realizar determinadas acciones, lista de amigos, tiempo de juego, o estado de ausente o conectado.

Resultado de la negativa a ceder los datos de la captura anterior (derecha). No permite completar el proceso de configuración, ni confirma que la verdadera causa es la no aceptación de la misma.



Ejemplo de consentimiento forzado para acceder a las funciones multijugador del videojuego.

2.2.2. Interés legítimo

El interés legítimo en los videojuegos, al igual que en muchos otros sectores se utiliza para legitimar tratamientos que responden a una utilidad corporativa que no daña los derechos y libertades del interesado, como por ejemplo, el control y gestión de la seguridad para evitar problemas en un servicio que utilizan de manera simultánea millones de jugadores[29], la prevención de trampas y conductas indebidas, la generación de estadísticas de jugador y logros, o incluir contenido que mejora o amplía la experiencia de jugador[30], siempre que se permita oponerse. Asimismo, se basan en esta vía de justificación los tratamientos ordinarios de gestión y atención al jugador o el envío de comunicaciones comerciales basada en la excepción del artículo 21.2 de la LSSICE.

Dentro de esta base también se plantean otros tratamientos sobre los que podría existir una serie de dudas de equilibrio dentro de la preceptiva ponderación de interés legítimo y sus criterios de necesidad y proporcionalidad. Por ejemplo, el tratamiento de targeting o segmentación publicitaria totalmente automatizada con ese objetivo de impactar comercialmente sobre el interesado, segmentar a los jugadores en función de sus gustos, o modificar ciertos aspectos del juego o fases que no ha sido populares, o reorientar expansiones y contenido postlanzamiento. En definitiva, crear una verdadera economía del dato[31].

[29] Elemento reconocido específicamente en el considerando 49 del RGPD.

[30] Ejemplos de estos son:
1) la lectura de los datos de guardado de partida o juegos almacenados de la tarjeta de memoria de la 1º consola PlayStation para generar el efecto de que un personaje del mismo tenía poderes telepáticos, en el videojuego Metal Gear Solid 1.
2)La posibilidad que se barajó en la versión de prueba (demo) del videojuego PT – Silent Hill para recopilar el correo electrónico real del jugador para enviarle mensajes en determinados momentos para aumentar la sensación de inmersión y terror psicológico.

[31] Aunque varias de las multinacionales que están detrás de los videojuegos de gran presupuesto, como Activision-Blizzard, Electronic Arts, Ubisoft, Capcom, Konami, Valve, Tencent Games o Nintendo no se las ubique al nivel y retos de privacidad de los grandes tecnológicas, lo cierto es que guardan muchas similitudes con ellas y son un campo de uso intensivo de técnicas de Big Data. Sin dejar fuera, que grandes tecnológicas como Microsoft o Sony tienen filiales especializadas que comercializan dos de las tres consolas de sobremesa más populares, y que tiene una fuerte capacidad de edición y adquisición de estudios; o que tres del selecto grupo «GAFAM», como son Amazon, Google o Facebook, han entrado en este sector millonario desde el streaming total con sus plataformas Luna, Stadia o Facebook Gaming.

Entrando en la valoración jurídica basada en el RGPD, específicamente en el artículo 6.1.f y el considerando 47 del RGPD, cabe recordar que el elemento nuclear es el triple juicio de legitimación, necesidad y proporcionalidad que debe quedar plasmado en la evaluación de interés legítimo, aunque sin olvidar, también, el hecho de que no exceda de las legítimas expectativas del propio interesado.

Del primer punto, no cabe realizar comentario debido a que no se tiene acceso a los informes de ponderación[32], pero con respecto a las expectativas de jugador, podría valorarse que no se encuentran dentro de lo que el usuario espera[33] porque no se concretan suficientemente esas finalidades legítimas buscadas por el responsable, más allá de expresiones genéricas como «optimización empresarial y de servicios», «análisis y segmentación de datos» o «entrenamiento y desarrollo».

Asimismo, las legítimas expectativas de un jugador medio (*alejadas completamente de la idea de privacidad*) está en un umbral mayor que en otros sectores, no por el conocimiento de los peligros y riesgos que pueda implicar para sus derechos, sino por la exigencia de que cualquier juego que se precie debe permitirle conectar con la lista de amigos sin necesidad de tener que introducirlos manualmente, recibir exclusivamente ofertas de juegos que le interesen, conectarse a varias plataformas sin tener que crear múltiples cuentas o autenticarse, o compartir capturas y contenido casi automáticamente en redes sociales.

2.2.3. Ejecución del contrato

i) Contrato en el que el interesado es parte

Esta base de legitimación parece está limitada a aquellos datos que sean necesarios para gestionar y ejecutar el contrato con el interesado, pero en ciertos casos se utilizan como forma de legitimación sobre tratamiento sobre los que pueden existir dudas, como, por ejemplo, el control parental, las promociones y concursos, la detección de abusos y trampas[34], o diversas funcionalidades del juego.

Entrando en la valoración jurídica, en atención al considerando 44, el artículo 6.1.b del RGPD, y las directrices del EDPB sobre esta base de legitimación[35] , muchos de esos tratamientos ejemplificados no encajarían en la propia ejecución del contrato, salvo aquel relativo al tratamiento de los datos necesarios para prestar el servicio contratado (*licencia*), y limitado a los datos de la compra y facturación del juego, incluyendo como recuerda el EDPB: «*la propia gestión del servicio postventa, garantía legal o laboral de administración o facturación necesaria tras la finalización del contrato*»[36].

Podría justificarse que todos estos tratamientos ejemplificados sobre los que existirían dudas, cumplirían con el elemento de ser contratos o acuerdos en los que el interesado es parte, pero se quedarían fuera del elemento de la propia necesidad para llevarlos a cabo, ya que este criterio debe interpretarse de manera restrictiva[37]. Es decir, sin que quepa todos aquellos tratamientos que no fuera objetivamente necesarios para

[32] Aunque sería recomendable en aquellos tratamientos más complejos enseñar una versión limitada en atención a responsabilidad proactiva, el propio RGPD no obliga a informar o dar transparencia de los mismos.

[33]Considerando 47 del RGPD y mención del ICO apuntando específicamente a este elemento en su guía general sobre el RGPD.

[34] En el punto anterior, relativo al interés legítimo, se ha comentado que la detección y prevención de trampas y abusos se encauzaba correctamente por la vía legítimo, pero no es algo unánime en los grandes actores de este sector analizados.

[35] «Directrices 2/2019 del EDPB sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados», de 8 de octubre de 2019.

[36] Punto 39 y 41 de las directrices 2/2019.

[37] El EDPB en las referidas directrices 2/2019, lo recuerda en su punto 19.

ejecutar el contrato, aunque si pudieran considerarse necesarios para que el responsable cumpla con un propósito corporativo determinado[38].

Además de este criterio más académico, se podría argumentar que, por el mero cambio constante en la tecnología del tratamiento y analítica de datos, especialmente por técnicas de Big Data, que se efectúa mientras está vigente el servicio la ejecución del contrato no sería la base adecuada para legitimar lo que está haciendo realmente.

Finalmente, el EDPB[39] nos recuerda que toda esa capacidad de influir en el usuario o «engagement» y las métricas que se recopilan en los servicios digitales, expresadas bajo expresiones como «mejora en el servicio», no procedería en ningún caso justificarlo por la vía de la ejecución del contrato.

ii) Medidas precontractuales solicitadas por el jugador

En relación con la otra posibilidad que permite el artículo 6.1.b del RPGD, cabe destacar un tratamiento que no se incluye en ninguna información específica de privacidad: la precompra o reserva de un videojuego. Generalmente realizada en formato digital a través de la plataforma a la que accedes para jugar, y consistente en que el jugador a cambio de una señal económica solicita que se aplique la medida precontractual de reservarle una copia de ese juego que no todavía no está en el mercado.

No podría considerarse que quedara cubierto por esta base el uso de un hipotético recordatorio o confirmación del e-mail para adjuntar publicidad u otro tipo de comunicación comercial no solicitada.

2.2.4. Obligación legal.

En este punto no se especifica nada al respecto más allá del concepto genérico de «obligación legal» o «cumplimiento normativo», por lo que no estaría cumpliéndose con el deber de información al no facilitar la norma específica que justifica esa obligación normativa para el responsable, y remitirse exclusivamente a la política de privacidad, y en la mayoría de casos, no dar una 1º capa informativa.

Como consecuencia de esa falta de información, debería incluirse la referencia a la ley concreta que obligaría al responsable al llevar a cabo ese tratamiento que exigiría el artículo 8 de Ley Orgánica de Protección de Datos y garantía de los derechos digitales, al determinar que deber tener rango de ley.

Debido a lo anterior, se puede hipotetizar en base a esta base legitimación, las cesiones típicas: fuerzas y cuerpos de seguridad en caso de investigación, tribunales, autoridades competentes en materia de consumo, sociedad de la información, o ámbito tributario (*AEAT*).

2.3. Transparencia e información

Uno de los grandes puntos a mejorar en materia de protección que tiene el sector de los videojuegos, es la provisión de la información de manera que permita cumplir efectivamente con el deber de información. Se opta por no dar ningún tipo de información base en primera capa, redirigiendo al usuario a una política de privacidad genérica.

[38] Criterio que se expresa en el artículo 7.4 del RGPD para delimitar la frontera entre consentimiento y contrato.

[39] Punto 48 de las directrices 2/2019 del EDPB sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, pág 14.

Como se ha referenciado en el apartado del consentimiento, lo más habitual es la pantalla de aceptación del contrato de licencia, junto con el enlace a la política de privacidad para intentar cubrir este apartado legal sin tener que ampliar el número de pantallas de configuración previa, y estableciendo una única casilla de opt-in para toda la documentación legal o texto mostrado. Posteriormente, por cualquier cambio ocasionado en materia de privacidad, se le vuelve a solicitar este consentimiento «*ómnibus*» del tratamiento junto con un enlace a la nueva política, pero sin informarle en ningún momento de cuáles son los cambios, o qué tratamiento son los que reamente legitimaría con ese «*consentimiento*» dado.

Cabe mencionar, aunque no es la fórmula habitual, se opta por ir un poco más allá del mero enlace y se incluye una pantalla propia de privacidad en la que se despliega la política de privacidad completa.

Siguiendo los considerandos 58, 60, 61 y 62 y los artículos 12, 13 y 14 del RGPD, así como en las directrices de transparencia del EDPB[40], lo dispuesto en la propia guía del deber de información[41], suscrita por tres de las cuatro agencias de protección de datos existente en España: Agencia Española de Protección de Datos, Agencia Vasca de Protección de Datos, y la Autoridad Catalana de Protección de Datos, cabe analizar punto por punto los distintos elementos de esta materia.

2.3.1. Transparencia

En relación con las obligaciones marcadas en el artículo 12 de que la información sea concisa, transparente, inteligible y de fácil acceso, cabe determinar que no lo es por los siguientes elementos. El comentario de la información relacionada con menores, se analizará en el apartado específico sobre ellos.

- **Concisión y transparencia**: aunque se muestra un enlace para acceder a la política de privacidad[42], no podría justificarse que eso sea suficiente para cumplir con el elemento de concisión por no separar completamente la información de privacidad de cualquier otra, o de transparencia por generar fatiga informativa o confusión el jugador[43], ni informar de los tratamientos específicos que se van a llevar a cabo (*solamente se incluyen ejemplos*). En este punto, el EDPB y el resto de autoridades nacionales, recomiendan específicamente dar esa información en capas,
- o incluso, a través de un panel de privacidad que sería factible incluir en este ámbito por ya existir para otras funcionalidades[44].

  Asimismo, sobre aquellos tratamientos con un fuerte componente automatizado, no se informe de las consecuencias o riesgos, por lo que el jugador que consultara la política antes de «*aceptar*», no podría hacerse una idea del alcance ni las consecuencias de los mismos[45].
- **Inteligibilidad:** en la información que se suministra en la política, se hace un esfuerzo visible en reconfigurar la denominación de los epígrafes usuales de la

[40] «Directrices sobre transparencia en virtud del Reglamento (UE) 2016/679» WP260 rev.01, de 11 de abril de 2018. Suscritas por el EDPB con su denominación previa al RGPD.
[41] «Guía para el cumplimiento del deber de informar» del 22 de mayo de 2018, suscrita por las tres autoridades citadas.
[42] Es habitual que la política mostrada es la misma que la recogida en la web del responsable, por lo que se referenciarán elementos que no aplican según la plataforma en la que se encuentre el jugador.
[43] Requisito que referencia el EDPB en sus directrices sobre transparencia en su punto 8.
[44] Especialmente recomendado en materia de servicios de la sociedad de la información, como sería el objeto del presente análisis.
[45] Punto importante referenciado en el considerando 39 y que forma parte del propio principio de lealtad del artículo 5 del RGPD.

información exigida por el RGPD, a otros términos más cercanos como «Qué hacemos con tus datos», o «con quién compartimos tus datos», aunque en la propia información se opte por no explicar con demasiada claridad determinados aspectos, como las finalidades, cesiones o transferencias internacionales[46], mezclándolo con la información con la relativa a cookies, o ocupando una parte muy significativa del texto con ejemplos de datos personales recopilados[47].

- **Facilidad en el acceso:** podría valorarse que este punto concreto se cumpliría en la fase de configuración previa al tratamiento porque, aunque no se informe claramente, sí que se facilita un enlace visible y funcional a la política de privacidad; pero no en resto del proceso al no estar disponible desde el laucher o app desde la que se accede al juego[48] [49]. La única forma de volver a acceder a la política de privacidad una vez que se ha aceptado, generalmente, es ir a la propia web a consultar la única versión que existe en el footer[50], o buscar específicamente la política.
- **Lenguaje claro y sencillo:** como se ha comentado anteriormente, el estilo es adecuado a la audiencia, obviando de momento el comentario sobre los menores de edad, aunque como ya se ha comentado, se utilizan términos abstractos, y se hace un intensivo de calificativo que plantean dudas sobre si se llevará a cabo o no, como, por ejemplo: «puede», «pueden» «posible» o «en *algunos casos*»[51].

Además, en algunos casos, al intentar incluir en un único texto varias especialidades en materia de privacidad de varios países, como son las del estado de California y el RGPD, referencian las siglas EEE, sin aclarar que se refieren a los estados miembros de la UE (*incluyendo transitoriamente al Reino Unido*), más Noruega, Islandia y Lienchestein.

2.3.2 Información

Como se ha mencionado, existe de manera generalizada una falta de la información mínima que se debe dar al jugador, bajo la premisa de que es suficiente con enlazar a una política de privacidad global radicada en la web. Para realizar el análisis de cada de las facetas de información, se va a seguir el orden marcado por el artículo 13 del RGPD.

i) Responsable del tratamiento, representante y delegado de protección de datos

En este apartado se cumple adecuadamente, tanto por la mención de responsable del tratamiento con los datos de contacto del mismo[52] (*generalmente la filial del Grupo*

[46] En el apartado de finalidades se incluyen referencias particularmente ambiguas en relación con el interés legítimo: «análisis y segmentación de datos», «segmentación de anuncios a través de contenido multimedia de pago»,

[47] Esta medida puede dar indicio de responsabilidad proactiva, pero al estar situada al inicio, distorsiona y dificulta que el jugador reciba la información marcada en los artículos 13 y 14 del RGPD.

[48] La matización de que la información que se suministra través de la app, debe a su vez ser accesible desde ella, responde a lo recomendado por el propio EDPB. Por lo anterior, tampoco sería aplicable que la información se encuentre a dos clicks desde la pantalla de inicio.

[49] Desde el launcher se puede acceder a varios apartados de configuración y un denominado «panel de privacidad», pero que en realidad se refiere a la posibilidad de hacer visible o no determinados parámetros como datos específicos del perfil, lista de amigos o comentarios.

[50] Elemento que rompería también la concisión de la información al no existir, generalmente, una versión específica para este launcher o aplicación de juego.

[51] En todas las políticas analizadas aparecen con una densidad bastante alta estos cuatro calificativos que el EDPB declara específica como improcedentes en sus directrices sobre transparencia.

[52] Se cumple lo dispuesto en la guía sobre el deber de información de las autoridades españolas (salvo la andaluza por no existir en su momento), al dar simultáneamente una dirección postal localizada y una dirección de correo electrónico específica.

empresarial a nivel europeo), o, también con la referencia específica y los datos de contacto del representante designado en la Unión Europea.

En relación con la referencia al delegado de protección de datos, se da un cumplimiento mixto al referenciarse solo en algunos casos su existencia y sus datos de contacto[53], a pesar de que, por la intensidad y naturaleza de los tratamientos llevados a cabo, entraría en el escenario de designación obligatoria por consistir su actividad principal en una observación habitual y sistemática de interesados a gran escala (*artículo 37.1.b del RGPD*). Se analizará en detalle en el apartado relativo a este elemento concreto.

ii) Finalidades

Bajo el epígrafe autoexplicativo de «Cómo usamos tus datos» se definen varias de las finalidades, con una claridad adecuada para las funcionalidades más ordinarias de la propia gestión de los datos, como las relativas a la gestión de la cuenta de jugador, transacciones o atención al cliente; pero con menor concreción en todas aquellas que realmente suponen un tratamiento automatizado, o totalmente automatizado en los términos del artículo 22, y se aportan ejemplos que pueden inducir a error con expresiones literales como las siguientes:

- «Gestionar nuestro negocio y personalizar y mejorar su experiencia de juego»:
- «Realizar investigaciones para la demostración y el desarrollo tecnológico»
- «Adaptarse a sus preferencias y entregar contenido dinámico»
- «Ofrecerle experiencias de juego que puedan interesarle»
- «Optimización empresarial y desarrollo de servicios. Realizamos operaciones de solución de problemas, investigación, análisis y desarrollo de productos y servicios para ofrecerle las mejores experiencias de juego y los mejores servicios»
- «Segmentación de anuncios a través de Paid Media» (*Medios de pago*) y "Custom Audience» (*Público personalizado*).

Principalmente, sería una omisión parcial de información que debe suministrarse al jugador para que sea capaz de comprender la naturaleza, riesgos y consecuencias de estos tratamientos más intensivos en datos y tecnología, es decir: referencia clara que suponen u decisiones automatizadas y elaboración de perfiles, la lógica y funcionamiento, las consecuencias para el jugador del mismo, y la posibilidad de oponerse o en su caso, el derecho a la intervención humana, a opinar sobre el tratamiento, y a impugnar esta decisión automatizada.

iii) Legitimación

Se mencionan las bases de legitimación que sería aplicables (*consentimiento, ejecución del contrato, interés legítimo y obligación legal*) bajo expresiones coloquiales como «Con qué motivos se utilizan sus datos» o «Cuáles son las bases legales para el tratamiento de datos», que permiten al interesado poder entender fácilmente el contenido que tendrán ese apartado concreto.

Los matices de cada una de las bases se han analizado en el apartado de bases de legitimación, destacando el elemento comentado de que se da una indicación general de obligaciones legales sin concretar cuáles ni indicar la norma de derecho europeo o con rango de ley[54] que las justifica, o que los intereses legítimos esgrimidos quedan muy

[53] La obligación de información del RGPD alcanza solo a los datos de contacto, habida cuenta de que la figura del delegado de protección no solo puede ser persona física, sino que puede también ser una entidad contratada para prestar dicho servicio.

[54] El artículo 8 de la LOPDgdd determina que los tratamientos basados en interés público u obligación legal deber estar reconocido en una norma de derecho de la UE o una ley.

difusos[55].

En ninguno de los casos analizados se informa de la obligación o no de facilitar datos y las consecuencias para el tratamiento de no hacerlo.

iv) Destinatarios

Se informa de manera muy general de los tipos de entidades a las que se les van a ceder los datos personales, sin aclarar la base legitimación utilizada para ello, y con expresiones generales no suficientemente concretas, como, por ejemplo: «proveedores *de servicios*» «colaboradores de marketing, filiales y empresas del Grupo», o «colaboradores de la plataforma»[56].

Aunque puede considerarse que cumplirían con este apartado, de conformidad a lo dispuesto en la guía del deber de informar[57] y el tenor literal del artículo 13 del RGPD, debería informarse claramente de aquellos destinatarios conocidos (*prácticamente todos en este caso*), y solo recurrir a especificar la mera categoría en casos extraordinario en los que realmente esa información pudiera cambiar con frecuencia o con la publicación de cada nuevo videojuego.

Sin hacer una mención formal y específica, y sin incluir una forma de consultar los encargados de tratamiento existentes[58], sí que se referencian, generalmente, con la expresión «proveedores de servicios».

Finalmente cabe mencionar que también es habitual que se referencia al resto de usuarios de la plataforma que interactúen con el jugador a través de alguna de las herramientas sociales puestas a su disposición, al ser teóricamente un tercero con acceso a los datos, aunque se encontrarían amparados por la excepción doméstica siempre que lo usen en ese marco de contacto social con otros usuarios, sin relación con actividad profesional o comercial[59].

v)Transferencias internacionales

En prácticamente todos los casos se realiza un enunciado genérico de que los datos serán transferidos cumpliendo con las garantías exigibles como las cláusulas tipo[60] o

[55] En ningún caso se cumple con la recomendación proactiva o buena práctica de incluir un breve extracto o resumen de la ponderación de dichos intereses, como indica la guía del deber de información española: pág 12, 1º párrafo.

[56] Puede ser referirse a desarrolladores y editoras del videojuego en concreto. También podría incluir a los llamados «modders» o personas que aceptan una licencia específica a para poder crear niveles o mapas a través de las herramientas para ello que se ponen a su disposición, y a los que podría darse acceso a datos de los jugadores que los hayan probado.

[57] Punto 7.4, 1º párrafo, pág 13: *«Cuando se haya previsto ceder o comunicar, legítimamente, los datos personales que se recogen, se informarán acerca de la identidad de los destinatarios, si están claramente predeterminados, o de las categorías de destinatarios, si estos no están determinados previamente»*

[58] De la propia definición de destinatario del artículo 4 del RGPD, se extrae que el encargado e tratamiento forma parte de este concepto por la expresión «sean terceros o no», por lo que estaría obligado el responsable a informar de ellos.

[59] Considerando 18 del RGPD: se hace una referencia específica al ejemplo de las redes sociales en el marco citado, y siempre teniendo en cuenta que el responsable que ponga a disposición de los interesados las herramientas sociales estaría obligado a cumplir con el RGPD en todo caso.

[60] A este respecto, no debe confundirse (*cosa que le pasó al autor de este análisis hasta que tras un comentario muy acertado de Francisco Javier Sempere en la red social Twitter, volvió a revisa el texto final del documento*) las cláusulas tipo en materia de encargado de tratamiento emitidas por la autoridad danesa (*standard contractual clauses january 2020 danish*), con unas cláusulas tipo del artículo 46.2 apartado c o b, ni con un contrato que habilite transferencia alguna: Punto 8.5 – pág 8.

decisiones de adecuación, pero sin concretar realmente a qué países se van a enviar los datos tratados, qué garantías concretas se aplican y dejándolo en condicional con expresiones como «en el caso de que se llevará a cabo».

En algunos casos, se informa de que los datos se transferirán a Estados Unidos bajo el acuerdo Privacy Shield ya anulado[61], y con la comprobación de que el responsable está dado de alta en el mismo, aunque se considera a Suiza[62] erróneamente como país con las debidas garantías y no se aportan los datos de la decisión de adecuación de la Comisión Europea que lo habilita (*solo la referencia al acuerdo de Privacy Shield especifica entre Estados Unidos y Suiza).*

No se hace referencia en ningún caso a normas corporativas vinculantes o BCR, ni a aquellos supuestos excepcionales de transferencias sin contar con garantías adecuadas[63]. Se mencionan mecanismos de certificación que ha obtenido el responsable, como, por ejemplo, las conocidas «APEC Cross-Border Privacy Rules», pero no se aclara si es una certificación válida en los términos de los artículos 42 y 43 del RGPD, y si realmente es un compromiso vinculantes y exigibles al responsable para que aporte garantías adecuadas al estándar europeo en este tercer país. En el apartado específico de transferencia internacionales, se analizará la situación tras la anulación del acuerdo de Privacy Shield.

vi) Plazos de conservación

Salvo en un par de casos de las entidades objeto de estudio, no se informa de plazos concretos, ni se especifican criterios para su conservación como marca el artículo 13, sino que se establecen enunciados genéricos como los siguientes:

«Conservamos sus datos durante el tiempo estrictamente necesario para llevar a cabo las operaciones para las cuales se han recopilado, salvo que la ley contemple plazos distintos».

«En caso contrario, conservaremos su información personal durante el tempo que sea razonablemente necesario para crear, mejorar y prestarle nuestros Servicios y cumplir la ley».

vii) Derechos

En este apartado existe un cumplimiento adecuado en todos los casos al concretar todos los derechos existentes en el RGPD y la posibilidad de reclamar ante la autoridad de protección de datos, dando una breve descripción de lo que son, cómo ejercerlos, generalmente, a través de la solicitud a una cuenta de correo específica, o por la cuenta de jugador/usuario, pero sin facilitar un modelo o formulario digital para ello[64]. En este último caso, no se solicita información acreditativa de la identidad, porque puede considerarse que el jugador ya está autenticado suficientemente por la propia cuenta e inicio de sesión.

---

[61] Anulado (Decisión 2016/1250) por el Tribunal de Justicia de la Unión Europea en la Resolución del Caso C-311/2018, de 16 de julio de 2020 (*conocida coloquialmente como Schrems II*).

[62] Primer país que contó con una decisión de adecuación al ser miembro del Tratado de Libre Comercio Europeo, pero no del Espacio Económico Europeo.

[63] El EDPS en el documento «Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling» sobre el conjunto de reglas a aplicar por la resolución del TJUE «Schrems II», de 29 de octubre habla de la figura de la evaluación de impacto sobre transferencias O «Transfer Impact Assessment» (*TIA*) para identificar si el tercer país tiene un nivel de protección equivalente al europeo.

[64] La referida guía del deber de información de la AEPD, determina en su epígrafe 7.5 de derechos que el responsable deberá informar claramente mediante modelos o formularios y explicando la forma de ejercer sus derechos al interesado.

viii) Procedencia de la información

No se cumple adecuadamente con este parámetro porque se incluye de manera genérica en la propia política de privacidad para evitar una posterior comunicación y sin aclarar el concepto de «fuentes de acceso público»[65]» de las que se van a obtener los datos, lo que puede provocar que se realice una extracción de información de redes sociales[66] del jugador sin que sea consciente.

ix) Información sobre datos concretos (proactividad del sector)

Como añadido propio del sector, cabe mencionar el gran interés por dar ejemplos concretos de datos personales tratados con listados que ocupan casi la mitad de la política, que, aunque no exigen se en el RGPD, podría ser una forma de mostrar responsabilidad proactiva en el cumplimiento.

El punto negativo de esta medida es que al ocupar tanto texto y situarse al inicio de la misma, puede provocar que el jugador no sea informado de los elementos que, si obliga el RGPD, y, por tanto, no pueda tener claro elementos como las base legitimación del tratamiento.

x) Ejemplos reales de los elementos comentados sobre la información dada al interesado

Ejemplo arquetípico de 1º capa informativa que mezcla términos y condiciones con privacidad, dando un mero enlace a los textos legales completos sin exponer la información básica preceptiva en 1º plano.

En la mencionada carpeta almacenada en nube se puede consultar copia de las políticas de privacidad analizadas para el presente estudio. Enlace a dicho repositorio: materiales.

2.4. Responsabilidad y corresponsabilidad

En la creación y explotación del videojuego, desde el punto de vista de la protección de datos, podría hablarse de tres actores principales:

- Estudio de desarrollo o desarrollador como persona física: creador efectivo del videojuego que actúa como gestor de los datos del título, tanto personales como técnicos o no personales.

[65] Antiguo concepto de la anterior LOPD, mencionado sin un desarrollo o aclaración de contenido en el RGPD, y no presente en la actual LOPDgdd.
[66] Las conocidas técnicas de data o web scraping.

- Editor y distribuidor del videojuego, conocidos generalmente como «publisher» en conjunto: titular de los derechos de explotación y de distribución del videojuego, que actuaría como responsable principal del tratamiento de los datos personales del mismo.
- Plataforma o launcher: sitio digital, generalmente con la misma estructura que una aplicación o plataforma digital, desde la que se accede tanto a jugar al propio videojuego, adquirir otros, acceder a contenido creado por otros jugadores, o utilizar funcionalidades sociales relacionadas, entre otras. Actualmente, es la forma hegemónica de acceder a un videojuego, por lo que este estudio se centrará en ella[67].

Las tres figuras pueden ser entidades independientes o formar parte del mismo grupo empresarial[68]. En el sector de los videojuegos, la cuestión de la responsabilidad se dirime totalmente por la vía de que todos son responsables independientes que se ceden datos según necesiten; pero teniendo en cuenta el concepto de la corresponsabilidad, así como lo dispuesto en las directrices sobre los conceptos de responsable, encargado y corresponsable del EDPS[69], cabría justificar que realmente pueden existir dos configuraciones de corresponsabilidad en varias operaciones del tratamiento:

- Corresponsabilidad entre el estudio que desarrolla el juego y la plataforma que acepta incluirlo en la misma.
- Corresponsabilidad entre la plataforma y el publisher, con el estudio de desarrollo como encargado del tratamiento de este último.

Antes de entrar a valorar cada supuesto, cabe aclarar dos elementos:

- Que la plataforma, salvo en el supuesto de que sea propiedad del publisher o de una empresa de su Grupo, caería dentro de la categoría de responsable (*corresponsable*) del tratamiento en atención a que no solo está en posición de determinar los fines[70], sino también de los medios a través de los cuales el jugador va a acceder al propio videojuego.
- La corresponsabilidad no lo es en todas las fases u operaciones de los tratamientos llevados a cabo[71], sino solamente en la recogida y cesión de los datos personales del jugador.

2.4.1. Corresponsabilidad entre el estudio y la plataforma que aceptar incluir su videojuego en la misma.

En este supuesto, no existiría la figura del publisher por lo que el estudio de desarrollo o desarrollador actuaría como responsable principal del tratamiento, y sería el que,

[67] Aunque los videojuegos suelen diferenciarse en tres grandes grupos separados por el hardware (*consola, ordenador y móvil*), esta figura es aplicable a los tres porque se utiliza en los tres ámbitos, ya sea de una manera más enmascarada con un sistema operativo ad hoc como en las consolas, o menos como en los otros dps casos con una aplicación o programa descargable al que acceder con usuario y contraseña.

[68] Lo más habitual en los videojuegos de gran presupuesto es que el publisher sea la matriz del Grupo, y a su vez tenga estudios internos de desarrollo (*conocidos como first party*), y una plataforma propia y exclusiva de sus videojuegos.

[69] «Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 1725/2018» - EDPS

[70] El EDPS recuerda en las mencionadas directrices sobre corresponsabilidad, que la determinación de medios y fines está relacionada, pero no estrictamente necesario que una parte determine ambos para poder ser considerado responsable del tratamiento – punto 3.1.3, 2º párrafo, pág 9.

[71] Dicha posibilidad de «corresponsabilidad selectiva» se enuncia en las Resoluciones del Tribunal de Justicia de la UE en los casos C-25/17 Jehovan todistajat y C-40/17 Fashion ID.

mediante acuerdo directo con la plataforma, decidiera incluir sus videojuegos en la misma.

En este caso existiría corresponsabilidad, y no una mera relación de responsable y encargado, al ser ambos los que determinan los medios, es decir, que le plantea al estudio en el acuerdo los medios a utilizar, y ambos determinan que el jugador pase por la plataforma como única vía legítima para jugar. Como se ha mencionado, serán corresponsables en la recopilación de los datos personales y la cesión de estos al estudio, con los subsiguientes tratamientos con responsabilidad exclusiva que este realice.

Aún en el supuesto en que la plataforma argumentara que únicamente es un sistema de intermediación con el jugador y que no trata dato alguno, en atención a lo establecido por el propio TJUE en varias resoluciones[72], no se determina como incompatible ser responsable y no tener acceso real o efectivo a los datos personales.

2.4.2. Corresponsabilidad entre la plataforma y el publisher, con el estudio como encargado del tratamiento de este último.

La única variación en relación a lo comentado en el punto anterior, es que el publisher ocuparía la figura del estudio, y este pasaría a ser encargado del tratamiento por cuenta de este. Será encargado de tratamiento, debido a que solamente tratará los datos (*y la gestión ordinaria y técnica del juego*), pero realmente no tendrá capacidad para decidir los fines o los medios en la medida necesaria para ser considerado responsable *(elementos esenciales)*[73], ni se le permitirá utilizar los datos fuera de las instrucciones dadas por el publisher como responsable y titular efectivo del videojuego.

En definitiva, sería el estudio, el que desarrolla la gestión del videojuego, con el apoyo como subencargados de las entidades que presten determinados servicios integrados en el videojuego, y recibirá estadísticas y datos anonimizados. El acceso al conjunto principal de datos lo tendrá como consecuencia de su posición como encargado de tratamiento.

Obligaciones conjuntas

De conformidad al considerando 50 y al artículo 26 del RGPD, la plataforma y el publisher, o en el otro caso el estudio, deberán suscribir un contrato de corresponsabilidad en que se delimite el alcance y la responsabilidad de cada uno en este punto concreto, especialmente en la información y ejercicio de derechos del interesado (*punto de contacto único*), así como el resto de obligaciones que aplicarán por el RGPD, como puede ser la gestión y colaboración en materia de brecha de seguridad, o la llevanza del registro de actividades de tratamiento

Aplicado al caso, y teniendo en cuenta la conocida Resolución Fashion ID, el deber de información le correspondería a la plataforma por ser la que tiene un contacto inicial con el interesado en todo ese proceso de apertura del videojuego antes de que aparezca la propia pantalla de inicio, informando de los elementos esenciales: existe una corresponsabilidad entre ella y el estudio o publisher exclusivamente en la recopilación y cesión de la información, punto de contacto para ejercer los derechos, y el resto de elementos del artículo 13.

[72] Wirtschaftsakademie Schleswig-Holstein C-210/16, Jehovan todistajat C-25/17, y Fashion ID C-40/17.

[73] En atención a que la determinación específica del medio a utilizar por el encargado, es decir de «los elementos no esenciales de los medios», no supone que este pase a ser considerado responsable. Por ejemplo, el programa para realizar un escaneo de la actividad del jugador y detectar el uso de programa maliciosos o trampas. Directrices 1725/2018 sobre los conceptos de responsable, encargado y corresponsable del EDPS. Punto 3.1.3, párrafo 6, pág 9.

El contrato de corresponsabilidad, en atención al modus operandi habitual del ámbito digital y lo mencionado por el EDPS[74], podría ser un anexo dentro del acuerdo de nivel de servicio (*SLA*) o un memorándum de acuerdo (*MoU*), y no necesariamente un contrato separado de corresponsabilidad totalmente formal.

2.4.3 Juego cruzado entre plataformas o «Crossplay»

Tradicionalmente, no ha existido la posibilidad en muchos videojuegos de permitir partidas entre jugadores de distintas plataformas distintas, es decir, que los jugadores que haya adquirido la versión A del videojuego porque tiene la consola A, puedan interactuar y jugador con aquellos que tienen la versión B porque poseen una consola B. Actualmente, tras la petición generalizada por la comunidad de jugadores, se está empezado a implementar este juego cruzado, que desde el punto de vista de protección no sería una cesión entre responsables, sino una verdadera relación de corresponsabilidad entre todos los responsables del tratamiento de esas plataformas distintas que acuerdan que sus jugadores interactúen en partida.

Se trataría de una relación de corresponsabilidad, en línea de lo que se ha expresado en el apartado anterior, porque los responsables del tratamiento de esas plataformas acuerdan los medios y los fines de ese tratamiento que permitirá el juego cruzado, es decir, que en sus plataformas se habiliten para permitirlo, con el intercambio y tratamiento cruzado de datos personales de los jugadores necesarios para que funcione el sistema[75]. Sin perjuicio de todos aquellos que se recopilen por analítica y control.

2.5. Encargado de tratamiento

En este punto no podría hacerse un comentario tan tangible porque el elemento de análisis existente son diversos modelos de contratos de encargado de tratamiento que cumplen formalmente con todos elementos dispuestos en el artículo 28 del RGPD, siendo en gran medida traslaciones literales del tenor de la norma.

Sí cabría mencionar que, junto con encargados de tratamiento de servicios ordinarios, tenemos varios específicos del sector con lo que debería suscribirse un contrato reforzado por la cantidad de datos personales, la naturaleza del tratamiento y el riesgo para los interesados. Asimismo, por la posición de riesgo en la que pondría al responsable del tratamiento por no seleccionar, como marca el 28.1 del RGPD, a un encargado que verdaderamente aporte garantías en medidas técnicas, organizativas y protección de los datos de los jugadores.:

- Analítica de datos: la prestación del servicio de big data tan común en el ámbito digital que, generalmente, se externaliza en grandes proveedores, como Amazon Kinesis[76] por tener la infraestructura necesaria para procesar en tiempo real una cantidad enorme de información generada[77]. Se analizará más en detalle dentro del apartado relativo a los tratamientos sometidos al artículo 22 del RGPD.

[74] El EDPS en el mismo documento, establece esta posibilidad de que el contrato adopte la forma de un SLA, o de un memorándum de acuerdo (*MoU*), pág 28, 2º párrafo.
[75] A modo ejemplificativo, y centrándolo en los datos estrictamente necesarios el nombre de usuario del jugador, dirección IP, dispositivo desde el que se accede, estadísticas e historial de jugador para poder computar las acciones dentro de la partida del jugador.
[76] Servicio prestado por Amazon como funcionalidad que se suma al servicio de almacenamiento de datos que provee bajo su filial especializada, Amazon Web Services. En el caso de la mayor parte de videojuegos de gran presupuesto y éxito es el proveedor más recurrente.
[77] El conocido Fornite: battle Royale necesita ocupar 12 datacenters del servicio de Amazon para poder gestionar un flujo de más de 90 millones de ventos por minuto. Se estima que el número de jugadores de este juego a nivel mundial ronda sobre los 70 u 80 millones, reconociendo oficialmente la empresa en mayo de 2020 la cifra de 350 millones de jugadores registrados.

- Sistema de antitrampas: el servicio tendente a evitar, por medios que en algunos casos pueden plantear dudas de proporcionalidad, que los jugadores puedan utilizar diversos programas que alteran el equilibro de la partida, como, por ejemplo, provocar lag artificial para evitar ser impactados o que el resto de jugadores no pueda defenderse, activar la visión a través de paredes, puntería perfecta o modificar el daño. Al igual que el anterior, es uno de los tratamientos más peligrosos y generalmente se recurre a proveedores especializados[78] por la cantidad enorme de datos y jugadores a gestionar simultáneamente. Se analizará también en el apartado sobre los tratamientos del 22.

Actualmente, ninguna de las asociaciones u organismos, tanto a nivel internacional, europeo[79] o español[80], que representan a los distintos actores del sector que actuarían como responsables y encargados de tratamiento, han optado por desarrollar un código de conducta aprobado por una autoridad de control competente en los términos del artículo 40 del RGPD[81], y cuya adhesión pudiera servir como una prueba de que el encargado goza de garantías suficientes para que el responsable le seleccione para el procesamiento de los datos (*artículo 28.5 del RGPD*).

Como ejemplo más reciente de un código de estas características, y del que podrían extraerse elementos válidos para cualquier sector, cabe mencionar el de la asociación NLDIGITAL, aprobado por la autoridad holandesa de protección de datos en agosto de 2020 en el marco de los contratos de encargado de tratamiento de cualquier empresa del sector TIC que se adhiera al mismo[82]. Como elementos a destacar:

- Exigencia de crear una declaración de cumplimiento del código para entregar al responsable del tratamiento dentro del proceso de selección del encargado del tratamiento, y como forma de generar prueba documental de que el responsable ha cumplido con su obligación de seleccionar a una entidad con garantías suficientes.
- Exigencia de mantener una política de privacidad actualizada y completa, dando un modelo de los elementos que debe tener en el propio código de conducta para facilitarlo.

2.5.1 Breve referencia a la delimitación del acceso a los datos personales en prestadores de servicios de intermediación en línea. Reglamento europeo 2019/1150

En atención a la aplicación efectiva el 12 de julio de 2020 del Reglamento europeo 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, ciertas de estas plataformas que se configura como servicios de intermediación en línea, tendrá la obligación de estipular

[78] Conocidos a nivel de nicho, pero con un alcance equivalente a algunos de los grandes servicios tecnológicos a nivel general: Easy Anti-cheat, Battleye (*PUBG, ARK Online o Conan Exiles*), FaceiT o Vanguard (*exclusivo del estudio y publisher, Riot Games*)

[79] En este ámbito tendríamos a la Federación Europea de Software Interactivo (*ISFE*), y a la Federación Europea de Desarrolladores de Videojuegos (*EGDF*)

[80] En España podría considerarse dos asociaciones principales en este ámbito que aglutinarían a los que efectivamente van a ser responsables y encargados del tratamiento de los datos de los jugadores: La Asociación Española de Videojuegos (*AEVI*) como organismo representativo de los editores y distribuidores (*aunque también incluiría estudios de desarrollo y desarrolladores autónomos*), y la Asociación Española de Empresas Productoras y Desarrolladoras de Videojuegos y Software de Entretenimiento (*DEV*).

[81] Teniendo en cuenta los elementos que el EDPB marca en sus directrices al respecto: «Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679»

[82] Data Pro Code van branchevereniging NLdigital (*denominación del código en holandés*).

en el contrato con usuarios profesionales (*estudios o desarrollares, en este caso*) el acceso a los datos personales y no personales que se llevará a cabo.

En particular, obligaría a todas estas plataformas que cumplan con los requisitos de intermediación online para usuarios profesionales y que la transacción sea directa entre estos y el consumidor[83], a incluir en las condiciones general de contratación el acceso técnico y contractual (*o la falta del mismo*) a los datos (*personales y de otro tipo*) que existirá en la prestación del servicio, tanto de la plataforma, como del usuario profesionales y del propio consumidor adquirente[84]. Concretamente deberán figurar los siguientes elementos típicos de un contrato de encargado de tratamiento:

- Los tipos de datos y las condiciones del tratamiento que el proveedor del servicio de intermediación hace de los usuarios profesionales. En caso de cesión a terceros no justificada para la ejecución del servicio, se deberá incluir la finalidad de dicha cesión y los mecanismos para que el usuario profesional se pueda oponer.
- Los tipos de datos y las condiciones del tratamiento de aquellos a los que tenga acceso el usuario profesional, incluyendo los generados en la prestación del servicio y los de los consumidores.
- Los tipos de datos y las condiciones de toda la información agregada, proporcionada o generada por la prestación del servicio, a la que tenga acceso el usuario profesional

Además de lo anterior, se establece la obligación del prestador que suspenda o termine el contrato, a devolver los datos al usuario profesional, incluyendo los que se hubieran generado en el uso del servicio antes de la terminación[85]. Esto aplicado a la parte de datos personales, supondría la entrega de los datos recopilados del usuario, pero también de los inferidos como si se tratará de un derecho de acceso en toda regla.

2.6. Destinarios y transferencias internacionales

En materia de destinatarios no haya una gran diferencia con el resto de sectores al cederse lo datos a un gran número a entidades comerciales y publicitarios (*cookies y tecnologías equivalentes*) con los que se tenga suscrito un acuerdo, y cabe la remisión a lo comentado en el apartado de información.

En materia de transferencias internacionales tenemos la anulación del acuerdo de privacy shield el pasado 16 de julio por el Tribunal de Justicia de la Unión Europea en el caso C-311/2018 (*conocida comúnmente como Schrems II*), es decir, el hecho de que Estados Unidos ya no es un país con las debidas garantías a este respecto. Esto supone que las transferenciales internacionales que tenga como destino dicho país se sitúan en un equilibrio delicado, ya que, aunque el TJUE declara que las cláusulas tipo de la Comisión Europea[86] [87] siguen siendo válidas, se exige adicionalmente el cumplimiento obligaciones adicionales para el responsable que exporte los datos:

[83] Este requisito en particular de la transacción directa entre el consumidor y el usuario, implicaría que no es de aplicación a las grandes plataformas del sector, como Steam o Epic, al realizarse la transacción por la propia plataforma y acordar un porcentaje o cuantía con el usuario profesional que pone la venta el videojuego.
[84] Artículo 9 del Reglamento (UE) 2019/1150.
[85] Artículo 4 del Reglamento (UE) 2019/1150.
[86] La relativas tanto para transferencia entre responsables y encargados, como entre responsables, recogidas en las la Decisiones 20001/497/CE, 2004/915/CE, y 2010/87/UE.
[87] La Comisión Europea ha publicado, el 12 de noviembre de 2020, un borrador de propuesta de decisión de una nueva versión de cláusulas tipo adaptadas al RGPD, para su consulta pública hasta el 12 de diciembre de 2020. Asimismo, se ha publidado en forma de anexo la propuesta de texto de propia cláusula tipo

- Realizar una valoración del estado de cumplimiento en materia de privacidad de país. Aunque se están dando pasos gracias a normativa estatales en esta materia, como las de los estados de California, Nevada o Maine[88], no existan norma a nivel federal que dé garantías. Se une que se trataría del 2º acuerdo sustentado por una decisión de adecuación que el TJUE anula.
- Aportar garantías contractuales adicionales para complementar a las cláusulas. En este punto, podría valorarse la utilización del contrato tipo de encargado de tratamiento (*artículo 28.8 del RGPD*) de la autoridad danesa de protección de datos, porque, aunque se declara específicamente que no puede utilizarse para justificar una transferencia, es un modelo de contracto de encargado adaptado al RGPD y validado por el EDPB que podría actuar como esa documentación de garantía adicional.

Esto trasladado al sector de los videojuegos, lo sitúa en una posición complicada porque lo habitual es transferir todos los datos a los servidores norteamericanos en los que almacenan y gestionan, y que ahora solo podría hacerse en los términos planteados[89]: con unas cláusulas tipo más las dos obligaciones enunciadas. Por el mero hecho de ser un tratamiento habitual, no cabría intentar ampararla por la vía de las excepciones del artículo 49 del RGPD, limitado a aquellas transferencias ocasionales y no repetitivas[90]. Como, por ejemplo, la mera asistencia a un evento o torneo específico, o la asistencia a un problema puntual en la cuenta del jugador.

Además del carácter no repetitivo y ocasional enunciado, no cabría justificarla por la vía extraordinaria del consentimiento explícito para intentar justificar esos tratamientos de analítica y segmentación o almacenamiento de la información, por la falta clara de libertad en dicho consentimiento y la obligación de informar del riesgo real al transferirlo a un estado no seguro que no cuenta con las garantías normativas pertinentes.

Cabe reseñar que es un tema en desarrollo que puede acabar con una posible nueva decisión de adecuación de la Comisión Europea a finales de 2020 o principios de 2021 que las legitime en términos similares a la situación previa a Schrems II. Asimismo, las autoridades norteamericanas competentes[91] han puesto de manifiesto, en un documento emitido a finales de septiembre de 2020[92] los límites teóricos y legales que existen en dicho país para que accedan las autoridades a esos datos procedentes de otros países. Sin entrar en detalle en el documento por no ser objeto del presente estudio, cabe reseñar dos ideas:

- No se realiza la captación y análisis de toda la información de compañías ni de los ciudadanos no norteamericanos que es transferida al país, en virtud a las dos normas que se mencionaban en la Resolución del TJUE (*Executive Order 12333 y Section 702 of the Foreign Intelligence Surveillance Act*); sino que se limita a lo dispuesto en el procedimiento existente para aquellos que puedan tener

[88] Gran parte de los estados de la costa este de Estados Unidos tiene proyectos de ley de privacidad en marcha: Nueva York, Pensilvania, Nueva Jersey, Rhode Island o Maryland; así como el medio Oeste: Minnesota, Iowa, Illinois, Wisconsin o Nebraska. En el caso de California, coincidiendo con las elecciones presidenciales del pasado 3 de noviembre de 2020, se reforzó la protección con la votación positiva de la ley de derechos de privacidad y cumplimiento (*conocida como propuesta 24*), y que viene a complementar la ley de derecho del consumidor ya en vigor.

[89] Salvo que la Comisión Europea en el ejercicio de su competencia apruebe una nueva Decisión de adecuación.

[90] Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679, de 25 de mayo 2018, pág 3 y 4.

[91] Departamento de comercio, departamento de justicia, y oficinal de inteligencia federal.

[92] Firmado por las tres autoridades indicadas: «*Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.*» Data Transfers after Schrems II.

interés para la seguridad nacional. La mayor parte de compañías e información no cumpliría con este requisito.
- Se alega que la Resolución Schrems II no se pronunció sobre si la protección de la privacidad en la legislación de los Estados Unidos, per se, era homologable a la europea o no.

Aplicada esta idea de que solo se accederá a la información que pudiera tener una relevancia para la seguridad nacional al objeto de estudio, cabría poner de manifiesto que los datos que traten los estudios o publishers podrían estar dentro de este análisis total de las autoridades federales, debido a que se ha teorizado con la posibilidad de que grupos terroristas utilicen chats y herramientas de comunicación de determinados videojuegos para ponerse en contacto[93], eludiendo a través de ellos gran parte de los controles sobre otros medios más usuales. Lo que en definitiva dificultaría, junto con los requisitos ya comentados, poder justificar la transferencia de los datos a Estados Unidos por ese posible acceso indiscriminado a todo el dataset con el objetivo de verificar la presencia de presuntas amenazas terroristas o de otra índole para la seguridad nacional.

Finalmente, en relación con transferencias a terceros en general, además de lo determinado en los artículos 44 a 49 del RGPD, se deberán tener en cuenta las recomendaciones del EDPB al respecto[94], emitidas para consulta pública el 10 de noviembre de 2020, y en las que se concretan la necesidad de analizar pormenorizadamente cada transferencia y la de colaboración activa y control del exportador e importador. Cabría destacar dos ideas principales:

- Las decisiones de adecuación no impiden a los interesados presentar una denuncia, ni a las autoridades de protección de datos llevarlo a un tribunal nacional para que remita una cuestión prejudicial al TJUE al respecto. Se pone como ejemplo el caso «Schrems I».
- Es necesario evaluar, en la línea de lo comentado en relación con Estados Unidos, el acceso a los datos que tendrán las autoridades de ese tercer país, con o sin conocimiento del importador[95].

2.7. Brechas y notificaciones de violaciones de seguridad

En este punto el sector de los videojuegos ha tenido una historia turbulenta de ataques a sus servidores, y que, en varias ocasiones, han supuesto brechas de seguridad de gran magnitud como, por ejemplo, la ocurrida en el sistema PlayStation Network/ consola PS3 de Sony en 2011[96] con la afectación de datos personales de 77 millones de jugadores, o en 2020 la acaecida en los sistemas de Nintendo con una afectación de más de 300.000 jugadores. El caso de Sony quedaría fuera del presente estudio por ser un episodio ocurrido varios años antes de la entrada en vigor del RGPD,

[93] En atención a las noticias publicadas sobre la investigación llevada a cabo en el marco de varios atentados terroristas ocurridos, aunque existe discrepancia entre sí ha ocurrido realmente o es una mera posibilidad hipotética. En cualquier caso, la mera posibilidad llevaría al control por parte de las autoridades federales, justificado por el posible interés para la seguridad nacional.

[94] Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE.

[95] Específicamente se referencia la existencia de precedentes, facultades legales, recursos técnicos, financieros o humanos. Asimismo, se incluye que se deba valorar la posibilidad de que se realice mediante interceptación directa del canal de comunicación de los datos.

[96] Reivindicada por Anonymous en represalia por un procedimiento judicial contra el autor de un conocido jailbreak del sistema de Playstation. Sin repercusión en datos personales, el también colectivo de ciberdelincuentes, Lizard Squad, ha conseguido en varias ocasiones que los servidores de juegos de la compañía dejen de funcionar, siendo la última vez en 2020 con afectación al conocido juego FIFA 2020.

pero da cuenta del alcance que puede tener un problema de seguridad ocurrido en un único gran actor del sector.

Cogiendo como elemento de análisis (*y ejemplo más ilustrativo de la actuación del sector en este punto*) la brecha de Nintendo por ser reciente y en plena aplicación del RGPD[97]; y de conformidad a los artículos 33 y 34 del RGPD, y las Directrices sobre la notificación de las violaciones del EDPB[98], puede analizarse lo siguiente:

- No es posible saber si la comunicación a la autoridad competente en materia de protección de datos se hizo en el plazo máximo de 72 horas desde que el responsable tuvo conocimiento, ya que no es un procedimiento que deba ser necesariamente público y que en un plazo idéntico de tres días se comunicó públicamente por Nintendo tras un reportaje que daba noticia de lo que había pasado. Tampoco se puede contrastar la existencia del registro interno obligatorio de violaciones, sean comunicables o no, pero es probable que exista, aunque sea por mero control y gestión.
- No es posible, tampoco, conocer si se ha informado específicamente a cada jugador afectado de manera individual como marca el RPGD salvo que sea objetivamente inviable[99] , pero el documento oficial que se ha puesto a disposición del público incluía la información que marca el artículo 34, salvo por el nombre y la dirección de contacto del DPD o de otro contacto pertinente de la empresa: descripción de lo ocurrido y sus consecuencias, medidas adoptadas por el responsable y otras que debería adoptar el jugador en su cuenta.
- La comunicación a la autoridad de control y al interesado procedería ya que solo existe un alto riesgo, sino que se ha producido realmente un daño a los derechos de los interesados en forma de ese acceso indebido a 300.000 cuentas, con posibilidad de que se use fraudulentamente la tarjeta registrada o la cuenta de PayPal asociada, en su caso.

2.8. Delegado de protección de datos

Como se ha indicado en el apartado de información, solo en algunos casos se hace referencia al delegado de protección, a pesar de que todos estos grandes responsables (y *el resto de características*) que son objeto de análisis en el presente documento, estarían obligados en virtud del artículo 37.1 apartado b del RGPD, en atención a que su actividad principal[100] implica una observancia habitual y sistemática[101] de datos

[97] En atención a la clasificación de violaciones de seguridad del antiguo Dictamen 03/2014 del Grupo de artículo 29, respondería al tipo de «violación de confidencialidad».

[98] Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, del 6 de febrero de 2018 del EDPB (*Grupo del artículo 29 en dicho momento*).

[99] La publicación de la información en la página web o redes sociales, no sustituye al deber de información personal a cada interesado afectado, siendo en el caso de una multinacional de este nivel, y por el elemento de que el correo electrónico es parte necesaria para abrir una cuenta de jugador, prácticamente imposible argumentar un esfuerzo desproporcionado. Siendo Nintendo una compañía con videojuegos muy enfocados a menores, debería suministrarse información adaptada específicamente para que entiendan la situación.

[100] Definidas en las directrices sobre los delegados de protección de datos del EDPB (*Grupo del artículo 29, en su momento*): pág 7, 1º apartado, y que implica entender por actividad principal aquella que sean necesarias para llevar a cabo la actividad a la que realmente se dedica la entidad. Al igual que el ejemplo del Hospital que propone el EDPB, no podría desarrollar la actividad o servicio al jugador sin realizar un tratamiento de sus datos personales.

[101] En cualquier de los significados que marcan las directrices citadas en la nota anterior, pág 9: *«que se produce de acuerdo con un sistema; preestablecido, organizado o metódico; que tiene lugar como parte de un plan general de recogida de datos; o llevado a cabo como parte de una estrategia»*.

personales de los jugadores a gran escala[102].

Asimismo, del tenor literal del artículo 37, todos aquellos proveedores de servicios en conceptos de encargado de tratamiento, incluyendo al estudio por el planteamiento realizado en el apartado de responsabilidad de que actúa como encargado de tratamiento, deberán designarlo por encontrarse en el mismo supuesto del 37.1.b.

Aunque con el tener literal del artículo 37 ya se determina que deberían nombrar un delegado de protección de datos, en atención al artículo 34 de la LOPDgdd deberían hacerlo, adicionalmente, por cumplir con el supuesto de punto 1.d: «prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio»[103].

2.8.1. Comunicación a la AEPD.

Aunque en virtud del artículo 34.3 del RGPD, estarían obligados a comunicar en un plazo máximo de 10 días la designación, nombramiento o cese del DPD, en el registro de la propia AEPD, se constata que solamente está inscritos los siguientes[104]:

- NINTENDO IBÉRICA, S.A.U.
- WARNER BROS. ENTERTAINMENT[105].
- SONY INTERACTIVE ENTERTAINMENT ESPAÑA S.A.

En el caso de Warner Bros y Sony se habilita un único delegado de protección para todo el Grupo, de conformidad a lo que permite el propio RGPD, mientras que la filial española de Nintendo opta por un delegado de protección nacional.

2.9. Evaluaciones de impacto

En atención al uso intensivo de tecnología que se realiza en el sector de los videojuegos, que en muchos casos es necesario para poder gestionar adecuadamente un servicio en el que simultáneamente concurren millones de jugadores, tenemos que muchos de dichos tratamientos deberían someterse a una evaluación de impacto previa.

En atención a que cumplirían con dos de los elementos reconocidos en el listado de supuestos sometidos a evaluación de impacto de la AEPD[106], sin perjuicio de que por la mera escala pudieran considerarse sometido a evaluación los siguientes:

---

[102] Aunque solo se limitara a todo el tratamiento y segmentación con el objetivo de generar los estadísticas y datos de juego, y mantener la seguridad adecuada del juego para evitar trampas y conductas contrarias a los términos y condiciones. En relación con la gran escala no sería necesaria valorar su existencia, ya que, de media, implica el tratamiento de muchos varios millones de interesados, aun cuando solo se tuvieran en cuenta los europeos.

[103] Salvo que el Ministerio de Consumo regule las denominadas «loot boxes o cajas de botín» (*micropagos con contenido aleatorio*) como una modalidad de juego regulado, no sería aplicable para todos aquellos responsables de videojuegos que las contenga, el supuesto del artículo 34.1.n de la LOPDgdd.

[104] Como se ha puesto de referencia en la introducción, España en el octavo mercado mundial por facturación, y eso supone, que todas las grandes entidades multinacionales analizadas (*y las que no*) tienen una filial española.

[105] Filial del Grupo Warner Bros y titular de la división especializada en videojuegos: Warner Bros Games

[106] Listado de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (*art 35.4 del RGPD*) de 16 de mayo de 2019. En este caso, no se menciona el listado paralelo de supuestos sobre los que debería realizarse una evaluación de impacto, por no ser aplicable. Como se determina en este documento (*enunciado por el propio EDPB en sus opiniones preliminares sobre estos listados nacionales*), la aplicación de dos o más de los criterios reflejados, conlleva la necesidad de realizar una evaluación de impacto del tratamiento.

- Tratamientos de datos de menores de 14 años: la mayor parte de los videojuegos «triple A» o de gran presupuesto de corte multijugador configurados como «Game as a service» en los que se centra este análisis, sacrifican elementos del ámbito adulto, como, por ejemplo, la violencia realista o la sangre, para que la calificación de edad del videojuego [107], es decir, que el público potencial baje de los 16-18 a los 13 años[108]. Por este hecho, el tratamiento de datos de menores pasa de ser algo extraordinario o residual a ser parte del flujo ordinario.
- Tratamientos que impliquen el uso de datos a gran escala: a pesar de que es un concepto valorable, por el número de interesados, tanto como cifra concreta, como por posible porcentaje de jugadores a nivel nacional, la permanencia en el tiempo del tratamiento, el volumen de datos y el alcance geográfico mundial, serían verdaderos tratamientos a gran escala[109].

Asimismo, en atención al tenor literal del apartado 3.a del artículo 35 del RGPD, tendríamos a aquellos análisis y evaluaciones sistemáticas del artículo 22, es decir, tratamientos totalmente automatizados que producen efectos jurídicos en unos casos, y que afectan significativamente de modo similar, en otros. Cabe citar los tratamientos que por su naturaleza y riesgo para los derechos de los interesados caerían dentro del artículo, y de los que se hablará con mayor detalle en su apartado específico:

- Sistema de antitrampas[110] y control del jugador para evitar conductas contrarias a los términos y condiciones *(conductas inapropiadas, tales como insultos y vejaciones verbales, acoso a través de herramientas sociales, entre otras*) o que produzcan una vulneración o alteración del sistema.
- Análisis del usuario a través de técnicas de Big Data para obtener un perfil de jugador, es decir, aplicar técnicas avanzadas y totalmente automatizadas de analítica para obtener conclusiones personales que permitan saber cómo impactarle comercialmente, o poder crear modelos precisos de jugador para diseñar un contenido o videojuego.
- Loot boxes o cajas de botín: los conjuntos de objetos digitales aleatorios que se pueden adquirir en determinados videojuegos, si excede de ser un mero algoritmo y tiene en cuenta el perfil del jugador o controla los premios para garantizar que el jugador gasta más o le toca algo para evitar que deje de comprar, es decir, que sea totalmente automatizado que produce un efecto significativo en el comportamiento económico del jugador al hacerle gastar más dinero del que tuviera previsto en un principio.

Finalmente, en atención a los criterios del listado de supuestos de evaluación de impacto de la AEPD, también tendríamos los siguientes:

- Sanción no automatizada: modalidad de ese tratamiento de sistema antitrampas mencionados, pero en el que el control no es totalmente automatizado, sino que

[107] Todo videojuego debe pasar por un proceso de valoración previa a la entrada en el mercado para asignarle una etiqueta visible de la edad mínima para poder jugarlo y la existencia de otros parámetros como la violencia. Este sistema de autorregulación se denomina PEGI, y se gestiona por la Federación Europea de Software Interactivo (*ISFE*), con sede en Bruselas, a través de dos entidades: Instituto Holandés de Clasificación de Medios Audiovisuales (*NICAM*) y el Consejo de Estándares de Vídeo (*VSC*).

[108] Esta edad no es aleatoria, sino que coincide con la etiqueta PEGI de 13 para poder llegar a esta franja de edad tan cotizada. El gran exponente por popularidad y número de menores jugando en la actualidad es Fornite: Battle Royale.

[109] Criterios de valoración utilizados por el EDPB (*Grupo del artículo 29 en su momento*), en sus directrices sobre delegados de protección de datos (*DPD*).

[110] Conocidos en el sector como «sistemas anti-cheats»

la revisión y decisión la toma una persona designada[111]. Este tratamiento ameritaría una evaluación de impacto debido a que cumplen con los siguientes supuestos de la lista de la AEPD: es un tratamiento que contribuye a la toma de decisiones automatizadas (*no totalmente automatizadas*), implica una observación y monitorización de la conducta de la persona denunciada, incluyendo metadatos para poder valorar la infracción (*tanto las pruebas aportadas por el denunciante como las comprobaciones posteriores sobre el perfil del denunciado y conductas en otras partidas*), y supone un tratamiento a gran escala por el volumen de los videojuegos objeto de estudio.

- Estadísticas de jugador y logros: el perfilado automatizado que se genera de la evaluación del rendimiento del jugador para extraer conclusiones y predicciones de efectiva en el juego, logros conseguidos, pericia para categorizar al jugador en una liga de mayor o menor nivel, o mostrar determinadas ofertas «exclusivas» asociadas al nivel de jugador y estilo de juego o configuración.

2.9.1. El advenimiento de los datos biométricos conocido como «biofeedback»

La utilización de datos biométricos no se da en el sector actualmente, pero en atención a la referencia de sensores de ritmo cardíaco y de sudor en la patente registrada de un mando de consola que salió al mercado en noviembre de 2020 al mercado[112] y la deriva de la mayor inmersión en realidad virtual cabe mencionarlo brevemente.

El objetivo sería medir el estado del jugador y seleccionar una u otra escena cinemática, otro nivel distinto, o intensificar ciertos parámetros para provocar tensión o sobresalto, y, por tanto, siempre que se limite a esto y esos datos no se registren o almacenen en ningún momento, podría justificarse que a pesar de que nos encontramos ante datos del tipo biométrico sería un tratamiento de datos personales exceptuado del cumplimiento del RGPD (*y de una evaluación de impacto*) en virtud al artículo 2.1 del RGPD[113].

Esto supondría que procedería entrar en el debate doctrinal sobre si el tratamiento de datos biométricos con la finalidad de identificación o de verificación/autenticación debe considerarse tratamiento de categoría especial en todo caso[114], o solo en los supuestos en los que el tratamiento sea de identificación como tal, es decir, ese proceso

[111] Muy habitual en videojuegos de corte multijugador que se ponga a disposición de los jugadores herramientas de denuncia de este tipo de conductas, mediante la grabación de pequeños clips de vídeo y posterior remisión a través del canal habilitado, o la posibilidad de etiquetar al presunto infractor en función al tipo de acto para su posterior investigación por el responsable. En algunos casos, como, por ejemplo, el del conocido Counter: Strike Global Offensive se permite que jugadores experimentados que acrediten un mínimo de horas de juego (*se presume un conocimiento profundo del juego y la capacidad de descubrir ciertos indicios de uso de hacks en partida*) puedan apuntarse al programa de revisión para poder ayudar al responsable a hacer una 1º criba de los clips de vídeo denunciados.

[112] El fabricante de los mismos no ha determinado que estas funcionalidades formen parte o estén activas en la versión comercializada del mando, sino que es una hipótesis en atención a la descripción de las funcionalidades del mando dualsense de la futura Playstation 5 en los esquemas e información de la propia patente.

[113] El matiz de que los datos no estén contenidos o destinados a ser incluidos en un fichero como elementos necesarios para que aplique el RGPD, se ha utilizado por autoridades de protección de datos, como la CNIL, para determinar que el control de acceso mediante la toma de temperatura por un dispositivo de infrarrojos sin contacto que no almacene el dato de temperatura en ningún momento ni de ningún modo, caería fuera de la aplicación del RGPD

[114] Postura mantenida por la Autoridad Catalana de Protección de Datos en su dictamen 21/2020.

de búsqueda de correspondencias uno a varios[115].

2.9.2 Reflexión sobre la personalización del personaje

Como se ha enunciado en el punto anterior, no se realiza actualmente un tratamiento de datos de categoría especial, pero cabe mencionar las opciones de personalización del personaje del jugador en algunos videojuegos, poniendo el foco en las crecientes opciones del espectro de identidades de género[116] que puedan existir en la actualidad, y que la propia comunidad de jugadores reclama.

En este sentido, no se expone que la mera inclusión de diferentes opciones de género suponga el tratamiento de datos de categoría especial del tipo de vida u orientación sexual, pero sí que en aquellos casos más minoritarios con algún tipo de analítica o asociación al perfil del jugador que lo ha elegido, podría implicarlo por ser una opción que, per se, filtraría a una parte muy significativa de los interesados.

2.10. Cookies

Gran parte de los tratamientos automatizados que se llevan a cabo se gestionan a través de cookies en su sentido más amplio, es decir, no solo aquellas más tradicionales, sino también las llamadas «tecnologías equivalentes» por todas autoridades de protección de datos que han desarrollado guías y directrices al respecto[117]. En definitiva, hablamos de cualquier sistema o técnica que almacene o recupere información de un dispositivo. En particular cabría destacar todos aquellas que tratan de analizar y seguir al usuario:

- ***Fingerprinting* o huella digital**: técnica que es capaz de identificar al usuario gracias a herramientas como javascript o flash, al asignarle un identificador único y considerar que cada dispositivo pertenece a una persona distinta, aun cuando compartan el mismo núcleo familiar[118]. En definitiva, al igual que una cookie analítica, realiza una monitorización de la navegación del usuario, pudiendo incluso captar el desplazamiento del ratón, las teclas pulsadas, o el sistema de bloqueo de anuncios utilizado. Al respecto, la AEPD publicó un informe en febrero de 2019 sobre esta cuestión[119].
- ***Tracking pixel* o *web beacon*:** técnica que inserta una imagen del tamaño de un pixel en formato html para poder detectar las interacciones del usuario sin que este se dé cuenta. El más conocido es Facebook pixel, y se utiliza también en los sistemas de mailing para poder remitirle un informe al cliente sobre cuántos usuarios han abierto su determinada newsletter.
- ***Cookie syncing*:** tecnología que permite reconstruir y volver a identificar al usuario que haya borrado la determinada cookie, a través del identificador que se asignó en un principio, y que se envió fuera del dispositivo a un tercero.

Entrando en el supuesto de estudio, y como se ha referenciado en el apartado relativo al consentimiento y al deber de información, no existe un consentimiento separado y

[115] Postura mantenida por la Agencia Española de Protección de Datos en su informe 0036/2020.
[116] El reciente videojuego de gran presupuesto, Cyberpunk 2077 incluye la posibilidad de personalizar totalmente al personaje en este sentido, y no solo en el aspecto de apariencia física.
[117] Por ejemplo, la definición dada en la guía vigente de cookies de la AEPD: *«cualquier tipo de dispositivo de almacenamiento y recuperación de datos que se utilice en el equipo terminal de un usuario con la finalidad de almacenar información y recuperar la información ya almacenada»*.
[118] El ICO en su guía sobre cookies «Guidance on the use of cookies and similar technologies», ejemplifica la siguiente información que se extrae, relaciona o infiere con esta técnica de huella digital: datos derivados de la configuración del dispositivo, datos derivados del uso de la red, CSS, JavaScript, cabecera HTTP, fuentes instaladas, uso de APIs o plugins instalados.
[119] «Estudio de Fingerprinting o Huella digital del dispositivo», de febrero de 2019

específico para cookies[120], ni se informa adecuadamente a través de 1º capa y un enlace al sistema de gestión de cookies, o a un sistema que permita mostrar esa información en un único panel o banner integrado.

Asimismo, en la pantalla en la que se intenta integrar todos los elementos legales y anudarlos un único consentimiento/autorización, se incluye un enlace que no redirigirse a una información detallada de cookies que se van a utilizar el launcher ni el juego como tal, sino a la política de cookies (*en algunos casos forma parte de la privacidad[121]*) de la web del responsable.

Lo anterior supone que no pueda concretarse si algunas de las cookies referenciadas en la web, realmente se aplican al launcher o al juego concreto al que quiere acceder, y que, por tanto, no se cumpla adecuadamente con esta materia, ni permita saber a ciencia cierta cuáles se utilizan.

En relación a la información concreta que se publica en esas políticas de cookies no específicas y generales de la web, cabría matizar lo siguiente:

- En muchos de los casos se referencia erróneamente que a través de las cookies no se tratan datos personales en ningún caso.
- En la propia web sí que existe un sistema de información de doble capa y panel de configuración que cumple formalmente con los requisitos en esta materia para cualquier usuario que acceda a la misma desde internet.
- No se referencia en 1º capa si se tratan de cookies propias o de terceros, no se determina de manera clara en la mayor de ocasiones que se va a realizar un seguimiento y análisis del comportamiento del jugador en todo momento, ni tampoco la existencia de publicidad comportamental.
- Se utilizan expresiones desaconsejadas y confusas como «proporcionarle la mejor experiencia posible».
- No se mencionan posibles transferencias de datos ni se informa, como determina el RGPD, de las garantías concretas que habilitan la misma (*o la excepción del 49 del RGPD*), ni los terceros países a los que se transmiten.
- No se concretan todas las cookies y tecnologías equivalentes, especialmente de terceros, aunque de la consulta de las licencias de uso de software externo que se integra en el videojuego se determina su existencia. Por ejemplo, diversas APIs, JavaScripts, generadores de uuid (*Identificador único universal*). En este tipo de supuestos, sería todavía más importante que el jugador pueda conocer las cookies que se aplica ya que prácticamente muchos de los tratamientos más intensivos y con un mayor riesgo para sus derechos se van a gestionar a través de todas estas cookies y tecnologías equivalente.
- Generalmente no se incluye el plazo de conservación (*o los criterios*) que deben concretarse en todo caso[122].
- En ningún momento se informa adecuadamente de la corresponsabilidad que en rigor existiría en muchas de ellas, en atención a lo dispuesto en la famosa Resolución Fashion ID.

[120] Consentimiento en el sentido estricto del RGPD, sin que quepa variaciones en base a la figura de seguir navegando junto garantías, debido a la reciente prohibición de dicha posibilidad en el vigente texto de la guía de cookies de la AEPD de junio de 2020.

[121] Como determina la AEPD en la vigente guía de cookies, la información de esta materia deber ir destacada y separada de los términos y condiciones de uso, y de la política privacidad. Punto 3.1.2.3, pág 22.

[122] Determinado concretamente por el TJUE en su Resolución C-673/17, conocida coloquialmente como «Planet 49». Asimismo, se referencia en la propia guía de cookies vigente de la AEPD.

- En la mayoría de casos se incluye un enlace que permite acceder a un listado de todas aquellas entidades que analizan y gestionan las métricas y comportamiento del jugador a través del análisis de los datos obtenidos con la utilización de las cookies, junto con un enlace en cada uno de ellos para revocar el consentimiento.

Todo lo comentado, sin perjuicio de futuros cambios o matizaciones introducidas por el Reglamento e-privacy en el momento en que finalmente se apruebe un texto definitivo y entré en vigor.

2.11. Reglamento Europeo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (Reglamento e-privacy)123.

Es una de los grandes problemas no resueltos en materia de privacidad por esa gran dificultad que parece existir entre las autoridades europeas y los actores del sector para cerrar el texto de uno de los Reglamentos Europeos hermanos del RGPD (*que debería haber sido aplicable desde el mismo 25 de mayo de 2018*), llamado a actualizar el régimen de las cookies a nivel europeo de ya veterana Directiva 2002/58/CE.

Como se ha mencionado en el apartado anterior, las cookies y tecnologías similares en el sector de los videojuegos son capitales por ser el vehículo a través del cual se consigue esa monitorización y control continuo del jugador, tanto para esas finalidades centradas en mantener la seguridad, prevención de trampas y gestión adecuada del título, mejorar la experiencia jugable o ampliarla; como el perfilado de jugador con fines comerciales.

No procedería hacer un análisis a luz de un texto por no ser definitivo, pero si cabe mencionar los principales elementos que podría afectar, y que han sido puesto de manifiesto a nivel europeo dentro del sector de los videojuegos en las recomendaciones emitidas por la Federación Europea de Software Interactivo (*ISFE*) a la presidencia del Consejo de la Unión Europea[124] (*conocido también como Consilium o Consejo de Ministros*):

- *Cookies:* reforzamiento del consentimiento e información. que ya de manera progresiva se ha ido afianzando en las sucesivas guías de las distintas autoridades europeas de protección de datos, así como en las directrices del consentimiento del EDPB.

  Justo en esta recopilación de información del dispositivo por cookies[125] , tal y como pone de manifiesto el ISFE, la posibilidad de recopilar datos de los dispositivos de los jugadores quede supeditada al consentimiento, pero exceptuando aquellos supuestos de recopilación de datos de analítica del dispositivo por ser necesaria para prestar el servicio de S.I, o para medir audiencia (*se entiende que, por motivos de prevención de trampas y seguridad, así como de analítica pura*).
- Privacy by design: obligación de configurar el sistema para impedir a terceros almacenar datos e información del dispositivo o terminal del usuario, y de información al usuario sobre las opciones de configuración de confidencialidad y privacidad establecidas dentro del proceso de instalación. Es una medida en la última versión del borrador del Consejo aparece suprimida.

[123] Los comentarios sobre el Reglamento e-privacy se van a realizar sobre la base del borrador del Consejo de la Unión Europea, de 8 de noviembre de 2019.
[124] «Proposal for an e-Privacy Regulation Recommendations for the Finnish Presidency» ISFE, septiembre de 2019.
[125] Artículo 8 de la propuesta de Reglamento e-privacy en su borrador de 8 de octubre de 2019.

- Considerando 11: propuesta de cambio de la actual redacción de considerando 11.a, para que se considere como «comunicación no interpersonal», no solo al chat de comunicación abierto y general a todos los jugadores, sino también a los restringidos a los jugadores que participan en una partida.

Unido a estas reclamaciones de uno de los organismos representativos de responsables a nivel europeo a nivel europeo, debería tenerse muy en cuenta los metadatos[126] que el Reglamento e-privacy introduce como una de las grandes novedades, y que en el sector de los videojuegos pueden tener una gran relevancia por la cantidad de información que se gestiona de manera totalmente automatizada para que el juego en línea funcione, y por la posibilidad de que sirvan para identificar al jugador.

2.12. Derechos

En relación con el ejercicio de los derechos recogidos en los artículos 15 a 21 del RGPD[127] (*acceso, rectificación, supresión, limitación, portabilidad y oposición*), existe en la gran mayoría de casos un procedimiento habilitado por medios electrónicos para ejercerlos[128], tal y como marca de manera prioritaria la norma[129], completamente gratuito y con plazos de contestación asequibles dentro del límite de 30 días ordinarios, sin recurrir a peticiones que justificarán el aumento de plazo a dos meses más. Asimismo, existen varios puntos en los que no se cumple de la manera más adecuada lo dispuesto en la normativa:

- Transparencia: en todos los casos de estudio se informa en la política de privacidad de cómo ejercer los derechos en materia de protección o la mera dirección a la que dirigirse para ello (*sin contar el punto ya comentado de que dicha política solo es accesible desde la web y no desde el launcher que se juega y accede*), pero dentro de las cuentas de jugador se incluye el apartado específico mencionado anteriormente de «privacidad» que no es tal, y que puede inducir a confusión.
- Identificación del solicitante y datos adicionales: por la estructura del sistema que exige autenticarse con la cuenta de jugador para jugar o acceder a cualquier funcionalidad cada vez (*salvo que se permita guardar la sesión*), este apartado podría considerarse que está cubierto sin necesidad de comprobar la identidad del solicitante con un proceso separado al efecto. Dicho lo anterior, en los casos en los que se opta por una mera dirección de correo electrónico y no un sistema de autogestión automatizada de derechos, especialmente sobre el derecho de acceso, se llega a solicitar en algunos casos datos excesivos que en ningún caso son necesarios para comprobar la identidad del interesado. A modo ejemplificativo: número de serie de la consola, varios dígitos del sistema de pago

[126] El Reglamento e-privacy al hablar de metadatos menciona los siguientes ejemplos de información que pueden contener: considerando 2: (…) *«números llamados, los sitios web visitados, los datos geográficos, lugar, la hora, la fecha y la duración cuando un individuo hizo una llamada, etc., lo que permite una precisa las conclusiones que deben extraerse con respecto a la vida privada de las personas involucradas en la comunicación, como sus relaciones sociales, sus hábitos y actividades de la vida cotidiana, sus intereses, gustos, etc.»*

[127] No se han considerado en este apartado los derechos de información y a no ser objeto de decisiones totalmente automatizadas por tratarse de manera separada, y por no ser parte formalmente del paquete general de derechos del interesado en términos cotidianos, a pesar de que también lo sean.

[128] Solamente en uno de ellos se remite desde la política de privacidad a un área de la cuenta de jugador que no permite ejercerlo de modo alguno.

[129] Además de la referencia del artículo 12, también se reconoce en el considerando 59 dentro del supuesto particular del que el tratamiento (y en este caso, la relación con el interesado), se haga por medios electrónicos.

adherido a la cuenta, o detalles de la última transacción realizada en la cuenta asociada[130].

- En relación con los menores de 14 años, no existen procedimientos que verdaderamente exijan comprobar la identidad de los progenitores o tutores legales a efectos del ejercicio de cualquier derecho. La problemática inherente a los menores de edad inferior a los 14 años que marca la LOPDgdd como límite para prestar un consentimiento propio, se comentará en el apartado específico sobre el tratamiento de datos de menores, asimismo, se propondrán varias formas de comprobar la edad del menor en el apartado de propuestas.

En relación con el ejercicio de los derechos propiamente dicho, y tomando como base las solitudes realizadas para valorar el grado de cumplimiento, cabe analizar el nivel de cumplimiento de cada uno.

2.12.1. Derecho de acceso

Todo el sistema y la información se enfoca en facilitar el ejercicio de este derecho, incluso en forma de autoejercicio a través de la descarga automática de una copia digital de la información desde la cuenta de jugador, pero con las siguientes carencias:

- La copia se limita a una exportación de los datos contenidos en la base de datos sin una estructura o reordenación que permita que el jugador pueda entenderlos realmente. Solamente en uno de los casos de ejercicio de este derecho se adjunta una leyenda, y no es plenamente funcional por darse los datos en bruto.
- La copia de información no cumple la exigencia de contenido al limitarse a los datos recopilados y observados (*generalmente, limitado al historial de partidas*), sin referencia alguna a los inferidos, es decir, a aquellas valoraciones y conclusiones personales obtenidas del resto de datos que completan la definición de máximos del artículo 15.3 de «datos personales objeto de tratamiento». Se toma como base la información, procedimiento y formatos del derecho de portabilidad.

2.12.2. Derecho de rectificación

Se cumple adecuadamente en todos los casos a través de un sistema de autoejercicio en la cuenta de jugador.

2.12.3. Derecho de supresión

Se cumple adecuadamente en todos los casos a través de un sistema de autoejercicio en la cuenta de jugador, similar al de rectificación, o a través de la remisión a la dirección de correo electrónico específica de protección de datos[131].

2.12.4. Derecho de limitación

Solo se reconoces específicamente en dos de los supuestos como derecho ejercitable con ejemplos legítimos de casos en los que se podrá seguir tratando esos datos limitados: ejercicio o defensa de reclamaciones u otros fines distintos de los limitados con consentimiento del jugador; pero sin concretar la correlación con los derechos de oposición o de rectificación, es decir, la posibilidad de solicitar esta «paralización» mientras se resuelven.

[131] A nivel interno el responsable deberá tener en cuenta el bloqueo de esos datos para evitar que se traten, de conformidad al artículo 32 de la LOPDgdd.

2.12.5. Derecho de portabilidad

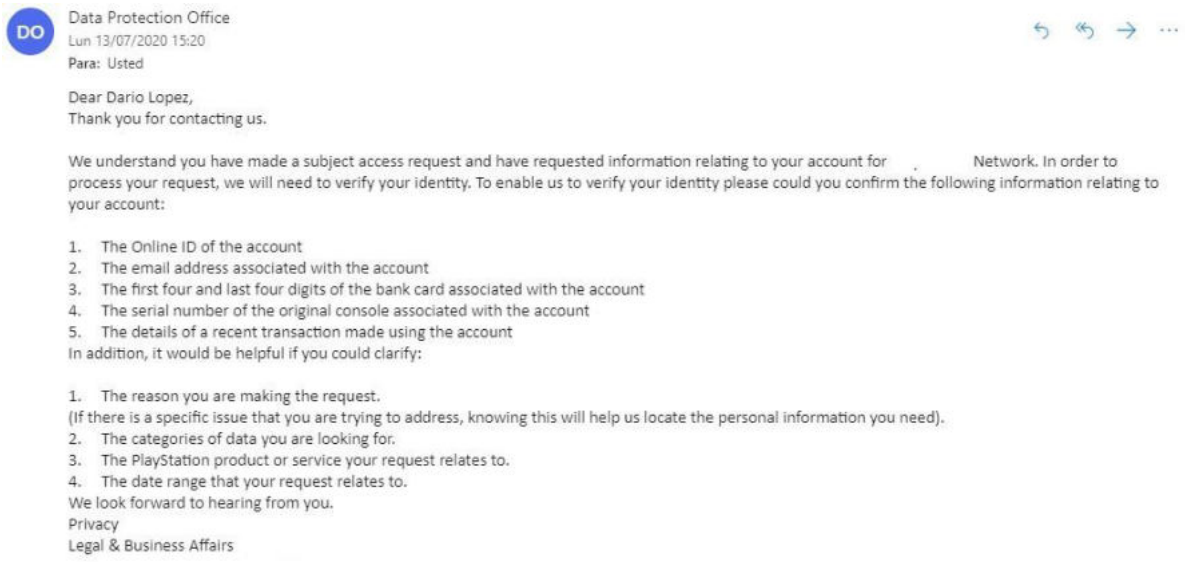
Se utiliza el mismo procedimiento e información que en el derecho de acceso, con la exclusión comentada de los datos inferidos en la copia de información[132]. Asimismo, se utilizan los mismos formatos en los que se entrega la copia de información, y que por ser generalmente XLX, Json o CSV, cumpliría con el requisito de darlo en un formato interoperable, de lectura mecánica y de uso común, solo en aquellos supuestos legítimos de portabilidad[133]

El problema es que no se permite al interesado decidir si los datos objeto de la portabilidad los quiere recibir o que se le remitan directamente al nuevo responsable, tal como marca el artículo 17 del RGPD, sino que al utilizar el mismo cauce que el derecho de acceso se le obliga a recibir personalmente la copia digital de la información.

2.12.6. Derecho de oposición

En todos los casos se permite el ejercicio del derecho de oposición, incluyendo la referencia al artículo 21.2 del RGPD de permitir al jugador oponerse a los tratamientos de mercadotecnia, como sería los envíos de newsletter o personalización publicitaria. Por contra, como se ha mencionado, no es habitual incluir la opción de oponerse al inicio del tratamiento, por lo que realmente no cumpliría totalmente con el elemento de «oposición en todo momento».

2.12.7. Ejemplos reales de elementos mencionados sobre el ejercicio de derechos



DO

Data Protection Office
Lun 13/07/2020 15:20
Para: Usted

Dear Dario Lopez,
Thank you for contacting us.

We understand you have made a subject access request and have requested information relating to your account for . Network. In order to process your request, we will need to verify your identity. To enable us to verify your identity please could you confirm the following information relating to your account:

1. The Online ID of the account
2. The email address associated with the account
3. The first four and last four digits of the bank card associated with the account
4. The serial number of the original console associated with the account
5. The details of a recent transaction made using the account

In addition, it would be helpful if you could clarify:

1. The reason you are making the request.

(If there is a specific issue that you are trying to address, knowing this will help us locate the personal information you need).

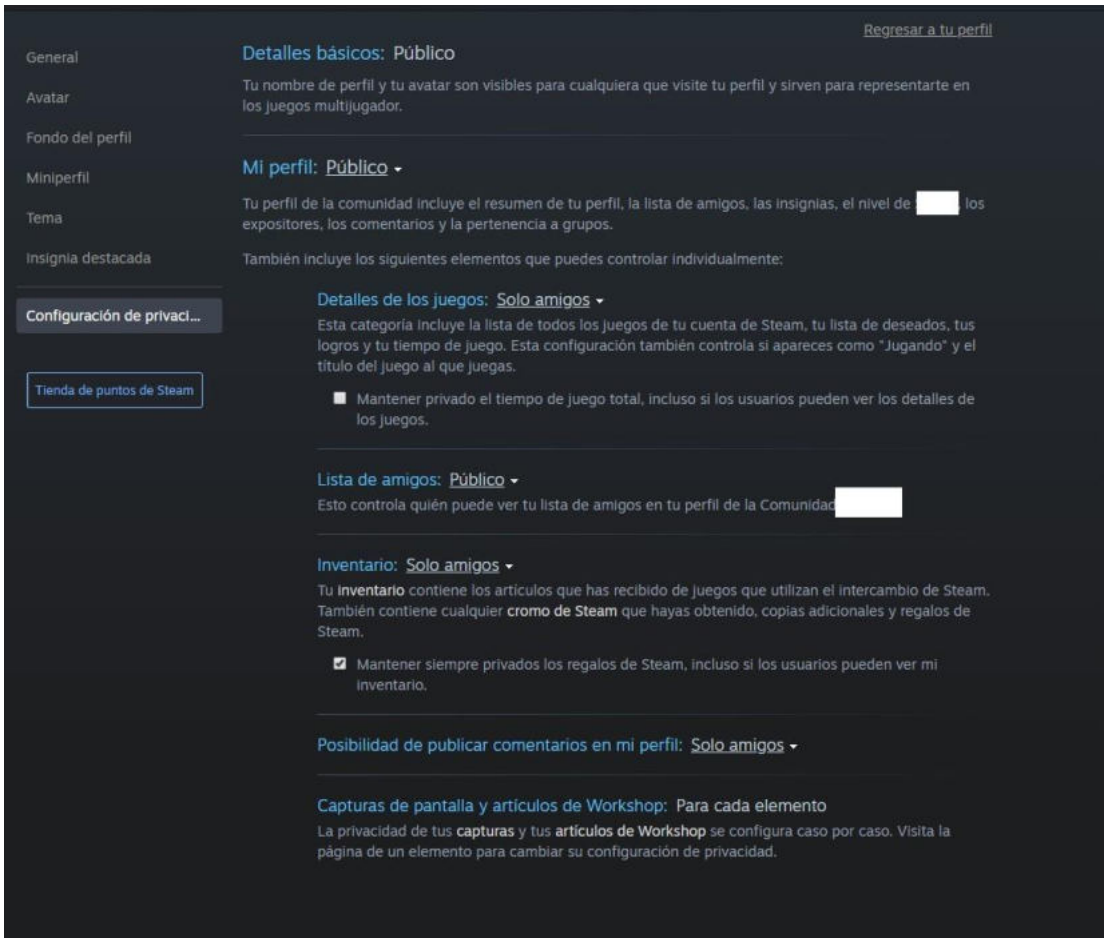
2. The categories of data you are looking for.
3. The PlayStation product or service your request relates to.
4. The date range that your request relates to.

We look forward to hearing from you.
Privacy
Legal & Business Affairs

Ejemplo de solicitud de datos de excesivos para comprobar la identidad del solicitante en el ejercicio de un derecho de acceso

[132] Las directrices sobre el derecho a la portabilidad de los datos del EDPB, de 5 de abril de 2017, (*en su momento Grupo de artículo 29*), determinan claramente que la portabilidad se limita a los datos recopilados y observados.

[133] Como marca el artículo 20.1 del RGPD se requiere la existencia de un tratamiento automatizado, y que se base en el consentimiento (*inequívoco o explícito*) o en la ejecución de un contrato.



Ejemplo del apartado típico denominado «de privacidad» pero no que permite ejercer derecho alguno en la materia, y solo configurar la publicidad de cierta información frente a otros usuarios de la plataforma.

2.13 Redes sociales

Las redes sociales son consustanciales a los videojuegos, especialmente en aquellos enfocados en el modo multijugador online, como son los videojuegos objeto del presente estudio. En particular, un videojuego «estándar» tendría varios tipos de herramientas sociales:

- Chat general: conversación abierta en la que cualquier jugador puede intervenir y ver los comentarios que se van realizando.
- Chat dentro de la partida: la forma habitual de comunicación con el resto de jugadores del equipo, o en su caso, con todos los jugadores de esa partida concreta.
- Chat personal con otros jugadores catalogados como amigos y chat privado de grupo.
- Diversos foros para compartir contenido, plantear debates o interactuar con otros jugadores, ya sea en general de la plataforma o limitado a un videojuego en concreto[134].

[134] Como uno de los ejemplos más completos, tenemos la pestaña o apartado de comunidad de la plataforma Steam por cada uno de los juegos que el jugador tiene en la biblioteca con el objetivo de que pueda compartir capturas, artworks, guías, participar en debates, compartir retrasmisiones, videos o noticias relacionadas.

- Herramientas de compartición y sincronización de contenido con diversas redes sociales.

Todos estos supuestos deben ser catalogados como redes sociales, por cumplir con los tres requisitos que marca el Comité Europeo de Protección de datos en su famoso dictamen 5/2009:[135]

- Cada usuario tenga un perfil con la información que el mismo haya suministrado.
- El contenido generado o cargado por el usuario (*fotografías, vídeos, comentarios, enlaces…*) se encuentre en línea.
- Posea un listado de contactos o usuarios registrados que permita la interacción entre ellos.

Unido a esto, en este apartado tendríamos uno de los tratamientos totalmente automatizados que producen afectos jurídicos sobre el usuario, al existir un control automático para detectar palabras consideradas como insultos, faltas de respeto, difusión de contenidos o propaganda de carácter racista, xenófobo, o de cualquier otro tipo que no proceda, con el objetivo de aplicar una determinada sanción al infractor[136]. En el apartado relativo a tratamiento del 22 se detallará más en profundidad, incluyendo el targeting o segmentación publicitaria por ser un tratamiento más amplio que no solo se utiliza en el marco de redes sociales.

Entrando en la valoración del cumplimiento de los elementos relativos a protección de datos en este punto, tendríamos varios puntos a destacar:

- Información: como ya se ha mencionado en el apartado 2.2.2, no se informa en 1º capa, y dentro de la política de privacidad única que se encuentra en la web no se dan detalles concretos de la recopilación de datos de redes sociales externas (*data scraping*) que se llevará a cabo en algunos casos. No se aclara lo suficiente en el apartado de finalidad, ni en los apartados propios del artículo 14 del RGPD, los tipos de datos y redes sociales concretas de las que se obtendrán datos en aquellos casos en los que se utilicen como forma de «autenticación rápida», para sincronizar la cuenta con las mismas para poder optar a premio, concursos o recompensas, o para enriquecer el perfil de jugador generado con técnicas de Big Data para fines de segmentación publicitaria (*targeting*)[137].

  Es este caso no existiría, en principio, tratamiento de datos personales de no jugadores que se encuentre dentro la plataforma por posibles descuentos y recompensas que se ofrezca a usuarios para traer a otros que no lo son, es decir, que fuera aplicable el artículo 14 del RGPD, ya que todos los datos son obtenidos necesariamente del propio jugador al abrirse la cuenta que le han recomendado.

- Privacy by design: a pesar de que se incluye el ya mencionado «panel de privacidad» con diversas opciones para poder restringir mensajes a la lista de amigos o lo que se puede ver en el perfil público de cada jugador, no se cumpliría

[135] Dictamen 5/2009 sobre las redes sociales en línea del Grupo del artículo 29, de 12 de junio de 2009.
[136] Podría oscilar entre la exclusión del chat por un tiempo, hasta el bloqueo temporal o permanente del acceso del jugador al mismo, es decir, al propio servicio contratado por el jugador.
[137] Mostrarle al jugador videojuegos que se ajusten exactamente a sus preferencias, incentivar la compra de determinados objetos virtuales sobre temáticas muy concretas que interesan al jugador; o de manera indirecta, utilizar los datos para enfocar el desarrollo de futuros videojuegos a modo de estudio de mercado infalible por el nivel de monitorización personales y detalle utilizados.

con el principio de privacidad por defecto del artículo 25 del RGPD al estar todas las casillas y opciones premarcadas en la modalidad más abierta de compartición y visibilidad posible. Es decir, contrario al punto 2 de dicho artículo en el que se exige que el responsable implemente las medidas necesarias para garantizar por defecto que los datos personales no sean accesibles a un número indeterminado de personas sin intervención del afectado.

En relación con la legitimación, cabrían hablar de dos posibles bases al respecto:

- Consentimiento: en relación con todas las herramientas sociales puesta a disposición del jugador, tanto internas como externas, ya que no podría justificarse por la vía de la ejecución del contrato por no ser estrictamente necesario para cumplir con lo contratado por el jugador, a pesar de que en aquellos en los que los jugadores se dividan por equipos ameritaría una herramienta de comunicación entre ellos. Dicho esto, existen ejemplo de herramientas de comunicación viables que no implican un chat o datos personales, como, por ejemplo, el denominado «sistema ping» de Heroes of the Storm[138], o las herramientas simples de dibujo sobre el mapa de juego de la Saga Total War en su modo multijugador para indicar acciones a otros compañeros o movimientos de cada uno de los miembros del equipo para coordinar la estrategia de batalla.
- Interés legítimo, más la posibilidad de autorización por ley del 22 del RGPD en relación con el control totalmente automatizado por motivos de seguridad, en los términos ya citados de comprobar que los jugadores usan la herramienta de los términos de la misma y de buena conducta citados.

2.14. Certificaciones

Además del ejemplo del código de conducta para encargados de tratamiento, impulsado por la asociación NLdigital y aprobado por la autoridad holandesa de protección citado, podrían existir otras certificaciones en forma, por ejemplo, de sellos o marcas, de conformidad al artículo 40 del RGPD. A efectos de servir como garantía del cumplimiento para un responsable o un encargado, en relación con los artículos 24.1 y .3, 25, 28.5, o 31 del RGPD.

En el sector de los videojuegos no existe ningún sello, marcas o certificación en materia de privacidad específico como tal[139], pero se empieza a utilizar el sello emitido por la entidad norteamericana, Entertainment Software Association o ESRB[140], en sus dos modalidades: cumplimiento en materia de privacidad, o cumplimiento adecuado en materia de menores en atención a la normativa norteamericana.

Aplicando lo recogido en los artículos 42 y 43 del RGPD, y las directrices sobre certificación del EDPB[141], cabría concretar que dicha certificación mencionada no

[138] Menú circular de cuatro iconos pulsables que señalan algo al resto de jugadores del equipo, incluyendo la marcación de algún punto en el mapa, que el jugador está en camino, la necesidad de cumplir un objetivo, o que hay un jugador rival en un punto concreto del mapa. En vez de reflejar el nombre de usuario del jugador, referencia el nombre del personaje que controla. Es cierto, que se incluye un sistema tradicional de chat y uno de voz opcional por petición especifica de los jugadores.

[139] Excluyendo del comentario la conocida certificación TRUSTe en materia de cumplimiento basado en el privacy shield que muchas empresas norteamericanas poseen.

[140] La misma entidad que en Estados Unidos se encarga de asignar una edad recomendada a cada videojuego antes de salir al mercado, al igual que en Europa lo hace la Federación Europea de Software Interactivo.

[141] «Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679», de 25 de mayo de 2018. Completado con un anexo en enero de 2019: «Annex 2 on the review and assessment of certification criteria pursuant

tendría un valor homologable en relación con el cumplimiento del RGPD, debido a que la entidad prestadora no está reconocida por ninguna autoridad de protección de datos nacional ni ninguno de los organismos nacionales de acreditación existentes, a nivel del EEE.[142].

Asimismo, no existiría transparencia suficiente, de conformidad a los dispuesto por EDPB en la referida guía, para determinar el objeto real de dicha certificación, más allá de su descripción general: «The Privacy Certified Seal demonstrates members' voluntary compliance with our rigorous program requirements»*;* y si se han tenido en cuenta los elementos básicos aplicables del RGPD:

- Bases de legitimación del artículo 6;
- Principios del tratamiento de datos en virtud del artículo 5.
- Derechos de los interesados conforme a los artículos 12 a 23.
- Notificación de violaciones de seguridad de los artículos 33 y 34.
- Privacy by design y by default del artículo 25.
- Realización de evaluaciones de impacto del artículo 35.
- Medidas técnicas, organizativas adecuadas del artículo 32.

A solicitud especifica de información a ESRB, se recibe como contestación que dicho sello/certificación es anterior al propio RGPD, y que, aunque se han incorporado elementos basados en el RGPD, no se encuentra aprobado por ninguna autoridad europea competente, ni se certifica el cumplimiento del RGPD, en modo alguno[143].

Finalmente, cabe concretar que, para facilitar el conocimiento de los mecanismos de certificación, marcas o sellos existentes, el EDPB tiene un registro especifico que es accesible desde su página web[144].

to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679»

[142] En España, ENAC (*Entidad Nacional de Acreditación*).

[143] Consultable dicha contestación, debidamente anonimizada, junto con el resto de documentación analizada en la carpeta en nube enlazada en la introducción.

[144] Actualmente, no figura ninguna entidad o mecanismo de certificación en el mismo, aunque deberá actualizarse con la referencia al 1º código que la AEPD aprobó e incluyó en su propio registro el 9 de octubre de 2020: «Código de conducta tratamiento de datos en la actividad publicitaria» de AUTOCONTROL.

3. Tratamientos especiales.

3.1. Menores

Uno de los puntos con un cumplimiento más laxo en el sector de los videojuegos, y en general, en toda la sociedad de la información por la complejidad que implica establecer un sistema fiable que impida que el menor acceda por sí mismo y que garantice que los padres o tutores legales han dado su consentimiento.

Como se ha mencionado en varios apartados de este estudio, existe una gran presencia de menores en los videojuegos[145] debido a que una parte significativa de los grandes videojuegos se diseñan pensando en poder incluir al rango de edad de 13 años[146]. Esto lleva a un gran riesgo para la privacidad y el propio el interés superior del menor[147], especialmente, si se tiene en cuenta las garantías adicionales que el considerando 38 recuerda a fin de cumplir adecuadamente con los principios de licitud, lealtad y transparencia, y no provocar un daño al propio menor[148]. Específicamente, lo siguiente:

- Mayor protección por ser menos conscientes de los riesgos y consecuencias del tratamiento.
- Mayores garantías en los tratamientos que supongan perfilado, tengan fines de mercadotecnia o servicios ofrecidos directamente al menor. En el sector de los videojuegos, tendríamos los tres tipos de supuestos.

Se podría centrar el análisis en cuatro grandes puntos principales.

3.1.1 Determinación de si el jugador es menor o no

En la gran mayoría de supuestos no se establece ningún mecanismo para intentar comprobar que el menor que está accediendo no tiene edad suficiente para dar un consentimiento válido por sí mismo. Lo más habitual es el sector son las siguientes modalidades de exención de responsabilidad:

- Transferencia de la responsabilidad del prestador del servicio a los padres o tutores legales: se incluye una mera referencia en la política de privacidad de que, si el usuario es menor, deberá el adulto al cargo aceptar las condiciones

[145] Según la Federación Europea de Software Interactivo, en su informe anual «In-Game Spending Study GameTrack Nov 2019», determina que aproximadamente el 75% de los menores de entre 6 y 15 juegan en al menos un dispositivo con regularidad, y que al menos el 36% de ellos realizan compras dentro de las mismos (*los conocidos micropagos por «skins» o «emotes» de Fornite, o de packs de cartas en la versión móvil del videojuego Fifa: FIFA mobile*).

[146] En relación con la anterior LOPD, la vigente LOPDgdd subió la edad de consentimiento del menor a 14, en consonancia con la edad fijada por la mayor parte de países europeos, dentro de la horquilla de 13 a 16 que permite el RGPD.

[147] El concepto clave que obliga a darle una protección más elevada para el menor. Aunque en la normativa sectorial e internacional, como por ejemplo la Ley de protección jurídica del menor, la convención sobre los derechos del niño de Naciones Unidas, o las Directrices de ACNUR para la determinación del interés superior del niño no se define como tal, podría expresarse como «mantener el bienestar del menor de la manera más amplia posible», es decir, en todos los ámbitos: seguridad, salud, bienestar, relaciones familiares, desarrollo físico, psicológico y emocional, identidad, libertad de expresión, y privacidad.

[148] En la nota técnica de la AEPD sobre protección del menor en internet en el acceso a contenido inapropiado, se reconocen parte de los riesgos para menores. Aplicados al sector de videojuegos, podrían darse los siguientes: desarrollos de conductas socialmente inapropiadas por la participación en chats y otras herramientas sociales del videojuego para una edad superior a la suya o sin un control adecuado, gastos económicos desproporcionados por aprovecharse de la menor percepción del menor, daños emocionales por frustración, o excesivo tiempo de juego de manera continua.

por él, y explicarle cualquier punto que no entienda de los textos legales del servicio.

- Autodeclaración del jugador de tener una edad igual o superior a 14 años: se utiliza el mero sistema de introducción de una fecha de nacimiento para generar una evidencia de que se ha implementado un sistema de control.

Entrando en la valoración desde el punto de vista de protección de datos, ninguno de los supuestos anteriores eximiría al responsable de su obligación de obtener el consentimiento válido, ya sea el de padres o tutores legales o del propio menor, y, por tanto, de poder determinar para ello si el jugador tiene al menos 14 años, con el límite del esfuerzo razonable o no desproporcionado[149]. Tampoco supondrían una evidencia real que permitiera demostrar que ha cumplido y que el consentimiento obtenido sobre el que se legitima el tratamiento es válido, tal y como pone de manifiesto el ICO en su código de buenas prácticas en el desarrollo de servicios online para menores[150].

Esta comprobación de la edad sería un tratamiento de datos personales autónomo y deberá cumplir con los parámetros del RGPD, especialmente en el caso de ser utilizada alguna técnica de perfilado para valorar la edad del menor, pero debiendo recabar el consentimiento separado de menor para utilizar dichos datos con otros fines., como podría ser mostrarle contenido publicitario personalizado o similares.

En el apartado de propuestas, se intentará aportar ideas tendentes a poder realizar esta comprobación de edad por medios telemáticos, a pesar de que es uno de los problemas que más dificultades genera en la sociedad de la información.

3.1.2 Información adecuada al menor

Siguiendo la pauta del apartado anterior, en el sector de los videojuegos no se da una información adaptada para menores, a pesar de que como recuerda el considerando 58, el punto 1 del artículo 12 del RGPD y el EDPB en sus ya mencionadas directrices sobre transparencia[151], el deber de información implica que el titular del derecho a la protección de datos reciba y entienda esa explicación de cómo se van a tratar sus datos[152]. Asimismo, el artículo 5 de la Ley Orgánica de protección jurídica del menor[153], determina que tiene derecho a recibir información adecuada a su desarrollo, que le permita actuar en línea con seguridad y responsabilidad y, en particular, identificar situaciones de riesgo derivadas del uso de las nuevas tecnologías.

La información que se suministra en la política general ya comentada, porque no se da otra distinta ni existen varias versionaes, está redactada de manera que pueda entenderla en su mayor parte un adulto, pero no un menor de edad. En atención a las directrices de transparencia del EDPB, el responsable que conozca que sus servicios son utilizados particularmente por menores/niños, debe redactar la información con un

[149] Establecer una medida enfocada a ese fin, en virtud al estado de la tecnología disponible y el riesgo existente. Como se ha mencionado, el riesgo en los videojuegos es mayor por el gran número de menores que juegan asiduamente.

[150] El documento «Age appropriate design: a code of practice for online services» de agosto de 2020 del ICO, en su pág 34, determina que la autodeclaración no produce una evidencia real y que solo se debería utilizar para tratamientos de bajo riesgo o cuando se utilice junto con otras técnicas.

[151] Punto 15, pág 46: *«En particular, el GT29 hace hincapié en que los niños no pierden sus derechos en materia de transparencia simplemente porque el consentimiento haya sido dado/autorizado por el titular de la patria potestad o tutela en una situación a la que se aplica el artículo 8 del RGPD.»*

[152] Punto 15, 1º y 2º párrafo, pág 11 de las directrices de transparencia.

[153] Ley Orgánica 1/1996, de Protección Jurídica del Menor, de 15 de enero.

vocabulario, tono y estilo de lenguaje adecuado[154]. Esto podría abrir la posibilidad de informar a través de iconos, dibujos, vídeos o símbolos, de conformidad a la idea de la información mixta entre iconos normalizados y texto que propone el artículo 12.7 del RGPD[155].

3.1.3 Obtención de un consentimiento real de los tutores o progenitores

Al igual que la información, no existe una práctica generalizada de obtención del consentimiento de aquel que completa la capacidad del menor. Solo en uno de los supuestos de estudio, se pone a disposición de los progenitores o tutores, una vez que se hubiera marcado en el botón de ser menor de edad, un formulario específico para autorizar la creación la cuenta del menor, con las funcionalidades parentales de control parental pertinentes

Como ya se ha mencionado, se diseña un sistema formal que intentar servir como prueba de cumplimiento adecuado, pero sin tener en cuenta los elementos comentados del RGPD y el ICO. Los responsables de origen norteamericano, incluyen la mención expresa en etiquetado digital y la política de privacidad de que cumplen con la normativa norteamericana específica: Children's Online Privacy Protection Act, conocida comúnmente como «COPPA».

3.1.4 Control parental

En todos los casos analizados existe un sistema de control que permite a los padres y tutores legales controlar el juego de los menores, estableciendo restricciones por edad, límites de tiempo, interacción en chats internos, o visualización del historial de juego.

No obstante, siendo un tratamiento de datos personales propio que monitoriza y controla al menor, solo en uno de los casos analizados se menciona en la política de privacidad dentro de los ejemplos de finalidades que se llevan a cabo. En ninguno de los supuestos se redacta de manera que el menor pueda entender qué implica realmente ese control parental.

3.1.5. Ejemplos reales de los elementos mencionados en este apartado

TÉRMINOS DE SERVICIO DE NETWORK

IMPORTANTE.

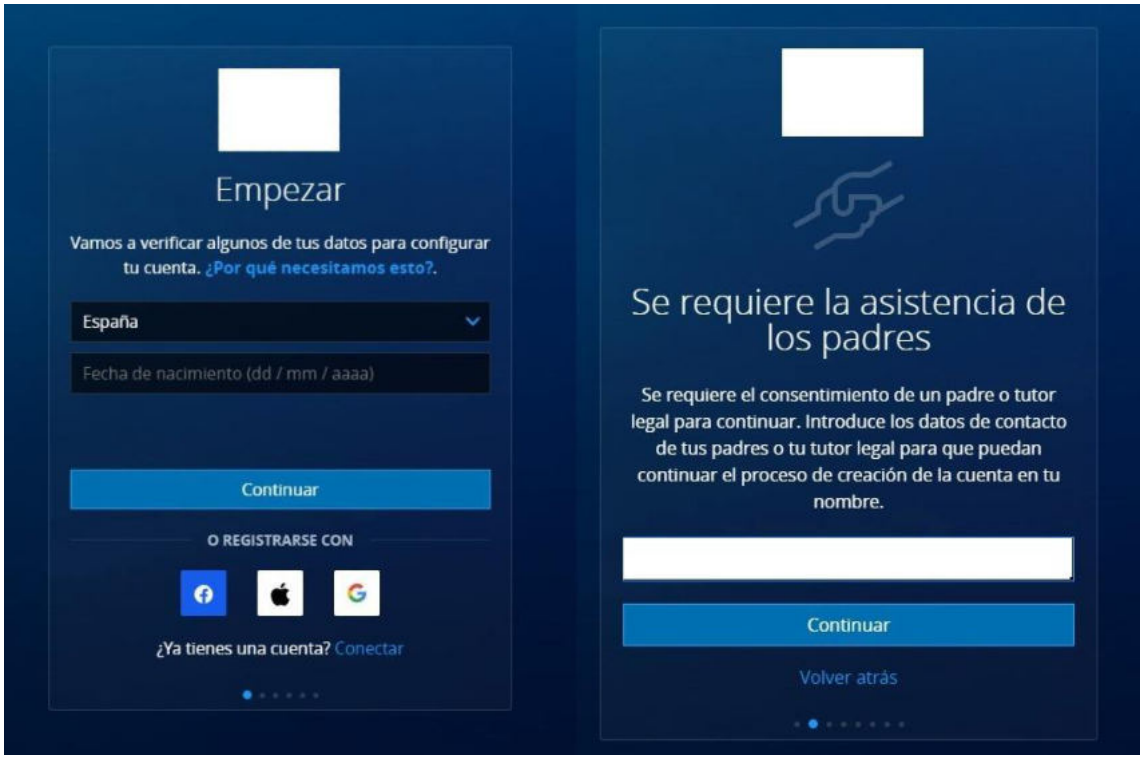
no es apto para niños menores de 7 años.

Si el usuario tiene entre 7 y 17 años de edad, su padre, madre o tutor legal ('**Adulto responsable**') debe leer y aceptar estos Términos en su nombre. El usuario también puede leerlos igualmente. El usuario debe pedir a su Adulto responsable que le explique cualquier cosa que no entienda. También puede consultar las Normas de PSN en [www. .com/legal/ Terms]www .com/legal/I Terms. Las Normas son más reducidas en extensión que estos Términos. Ayudan a comprender las partes más importantes.

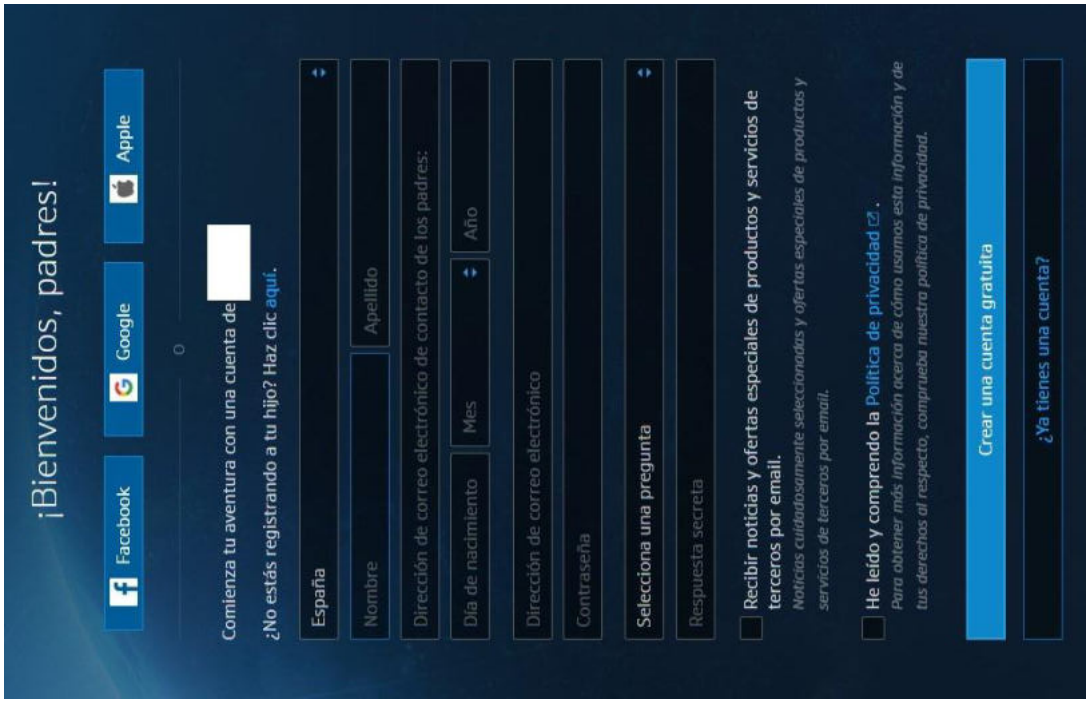
[154] El ICO en el mencionado código de buenas prácticas para el desarrollo de servicios digitales para menores, establece una serie de recomendaciones sobre cómo mostrar la información de los artículos 13 y 14 a menores, dividiéndolas por franjas de edad. págs. 41 y 42.

[155] Aunque el RGPD está hablando de iconos normalizados derivándolo a la determinación y autorización por la Comisión Europea a través de un acto delegado, y el EDPB no es muy partidario de su uso en las mencionadas directrices de transparencia, el artículo 12.7 no cierra esta posibilidad que tan bien podría encajar en el sector de los videojuegos. Por ejemplo, en la gran mayoría de los títulos de la conocida Nintendo que se enfocan a un público infantil.

Ejemplo de transferencia de la responsabilidad a los padres o tutores legales del menor reflejado en los propios términos y condiciones del servicio.



Ejemplo de un sistema de verificación de edad formal que no actúa como un control real que evite que el menor pueda pasarlo sin acudir a sus padres o tutores. Aunque en el 1º caso marque su edad, en el 2º lo único que tendría que hacer sería una cuenta de correo electrónico nueva para autorizarse a sí mismo el acceso.



Ejemplo de un formulario para padres o tutores legales en la creación de una cuenta para un menor, aunque sea un control que puede ser fácilmente superado por el menor.

3.2. Decisiones automatizadas y elaboración de perfiles. Incluyendo Big Data y sistemas antitrampas

Cabe analizar, como se ha anunciado a lo largo del presente estudio, los tratamientos más intensos y con mayor incidencia sobre el jugador que se llevan a cabo en el sector de los videojuegos: elaboración de perfiles[156] y decisiones automatizadas, tanto en sus versiones ordinarias[157], como en sus modalidades del artículo 22.

Son tratamientos que se llevan a cabo sin dar una información suficiente al usuario, con la única salvedad en casos muy contados de expresiones sucintas y no aclaratorias en la política de privacidad como «personalización de contenido»[158] sin que el usuario sea consciente de ellos ni de su alcance, y sobre los que pueden plantearse dudas relativas a la base de legitimación y si su alcance es adecuado al RGPD y LOPDgdd.

En relación con la elaboración de perfiles, hablamos de la monitorización y posterior análisis de elementos como el tiempo de juego, la franja horaria en la que se juega, el género de los títulos que tengamos en la biblioteca, el mayor uso de un personaje, equipo o mecánicas, preferencia del modo 1º jugador o multijugador, o el historial de compras; con el objeto de generar un perfil de jugador que determine el género y modo de juego preferido, la capacidad económica o predisposición a comprar un determinado juego o género, o, incluso para afinar, cancelar o sustituir contenido postlanzamiento del juego y evitar posibles fracasos económicos. Lo anterior, implica que esa monitorización o tracking sobre el jugador sea continua durante todo su período de juego, tanto en los menús de selección (*perfil de jugador o configuración de la tienda*), como en la propia partida; y que se apliquen técnicas de big data[159] para poder gestionar y analizar una cantidad de información tan alta[160].

En relación con las decisiones automatizadas, tendríamos tratamientos concretos como la prevención de trampas y expulsión automática, o tras una verificación humana, del jugador.

Finalmente, en relación con la modalidad del artículo 22 del RGPD, tendríamos que todo lo anterior suele estar totalmente automatizado por la imposibilidad de gestionar de manera manual o con intervención humana en el proceso

3.2.1. Tratamiento de elaboración de perfiles y decisiones automatizadas llevados a cabo en el sector, en atención a su finalidad.

Entrando a valorar más en profundidad estos tipos de tratamientos con una gran incidencia en la privacidad de los jugadores, podría desglosarse en tres tipos atendiendo

[156] Siguiendo lo determinado por el RGPD y las directrices sobre decisiones automatizadas del EDPB, por elaboración de perfiles se haría referencia a los supuestos.
[157] Aquellas que no cumplirían los requisitos que exige el artículo 22 para considerarlas sometidas a las al mismo, es decir, no se encuentra totalmente automatizadas, o que no producen efectos jurídicos o significativamente similares en el interesado.
[158] Solo en uno de los casos se hace una mención un poco más detallada al targeting y sistemas utilizados con las siguientes expresiones: «Segmentación de anuncios a través de Paid Media (medios de pago)», o «Custom Audience (Público personalizado) (sus datos personales sin cifrar nunca se comparten con terceros sin su consentimiento)».
[159] No es el objeto del presente estudio, pero realizando una definición libre se puede conceptualizar como: «el análisis automatizado a través de algoritmos específicos de grandes cantidades de información para extraer patrones y conclusiones.
[160] Como se ha mencionado en una de las notas previas en relación con el supuesto específico de Fornite, supone el tratamiento de 90 millones de «eventos» por minuto.

a su finalidad, valorando, asimismo, las posibles bases de legitimación a través de las podrían justificarse.

i) Información para mantener la seguridad, prevención de trampas y gestión adecuada del título

Este tipo de profiling no está enfocado en la captación de datos personales con el objetivo de generar un perfil que utilizar posteriormente, sino en la monitorización continua del videojuego y del propio jugador, de manera totalmente automatizada[161], para mantener la seguridad, un funcionamiento adecuado, así como prevenir cualquier tipo de trampas o conductas prohibidas.

- **Funcionamiento adecuado del título:** con el propio fin de que el servicio no presente ningún problema que pueda afectar al videojuego, se realiza una monitorización continúa del mismo para poder detectar problemas técnicos o exploits[162]. El objetivo no es la captación de datos personales sino el análisis de la información técnica, pero indirectamente supone un tratamiento de datos personales[163].

- **Mantenimiento de la seguridad y prevención de trampas:** este profiling sí va enfocado a individualizar al usuario para prevenir trampas, alteraciones del código, problemas en los servidores o vulneración de las normas de conducta de los típicos canales de chat. La monitorización no solo se centra en el comportamiento del jugador en el momento del juego, sino también en elementos más técnicos, como instalación de bots o hacks[164], variaciones anómalas de su conexión a internet para provocar lag artificial, uso de mandos o sistemas de juego no autorizados en la plataforma por razones de equilibrio, entre otras.

  La prevención de trampas se realiza a través de sistemas de escaneo del dispositivo desde el que accede el jugador, suponiendo una intrusión indebida en el derecho a la privacidad del jugador porque ese rastreo, totalmente automatizado del que se no se informa adecuadamente y que impediría en el caso de dar negativo acceder al juego o ser sancionado, se realiza sobre todos los archivos del dispositivo en busca de cualquier elemento que puede suponer un problema. En las versiones menos invasivas implicaría un escaneo continuo durante el tiempo de juego, y en el resto, uno que se realiza en todo momento.[165]

---

[161] La automatización total no se basa exclusivamente en una decisión corporativa de realizarlo de este modo, sino que debido a la gran cantidad de usuarios y datos simultáneos que se procesan para que un videojuego de gran éxito funcione correctamente, no sería viable hacerlo con intervención humana para garantizar un servicio que de tener un funcionamiento continuo sin interrupciones para permitir el juego.

[162] Fallos presentes en el videojuego que son aprovechables por los jugadores, sin necesidad de realizar ningún tipo de modificación técnica o alteración.

[163] En línea con el Reglamento europeo de datos no personales, habría que tener en cuenta la obligación de aplicar el RGPD al conjunto de datos en los casos en que no sea posible disociar la información personal de la estrictamente técnica o anónima.

[164] Alternaciones indebidas de ciertos elementos del juego que le confiere al jugador infractor ventajas muy significativas sobre el resto, como, por ejemplo, un input lag en la partida o en la experiencia del resto de jugadores que haga muy difícil dañarle, vista a través de obstáculos, apuntado automático, o modificadores de daño.

[165] Todos los grandes proveedores de este tipo de sistemas antitrampas, conocidos como anti-cheats (*Easy Anti-cheat, Punkbuster, Battleye, o FaceIT*) implican un escaneo totalmente automatizado del dispositivo desde el que accede el jugador. Debido a que dichos sistemas tienen un rango de efectividad limitado, se empieza a optar por versiones que supone una mayor invasión al escanear en todo momento el dispositivo. Por ejemplo, el llamado « Vanguard»

> Actualmente, se plantea aplicar a la selección de partidas entre jugadores de un nivel similar («matchmaking»), un filtro para clasificar a los jugadores en función de su «comportamiento», y concentrar a todos aquellos considerado tóxicos por su historial de sanciones, denuncias o reclamaciones, en una misma partida separada del resto.[166]

Desde el punto de vista de la legitimación, cabría determinar que de las bases que podría aplicarse[167], solo podría justificarse por interés legítimo[168], ya que el consentimiento implicaría una aplicación ineficaz por el hecho de que deba aceptarlo el jugador y que se dé una verdadera libertad en el mismo, el contrato que fuera un tratamiento estrictamente necesario para dar cumplimiento al mismo, y la obligación legal que estuviera exigido por una norma con rango de ley.

Este interés legítimo debería pasar por la evaluación de interés legítimo pertinente para determinar realmente si es un tratamiento necesario para la empresa con el objetivo perseguido, y si es proporcional y limitado a la finalidad concreta de prevenir las trampas y mantener la seguridad.

Salvo en aquellos casos en los que se realice una valoración final por un equipo de personales designado para tomar la decisión final sobre la sanción, al tratarse de un tratamiento totalmente automatizado., además de ese interés legítimo y una evaluación de impacto por imperativo del artículo 35.3.a, debe cumplir conjuntamente con una de las excepciones que el artículo 22 del RGPD establece para levantar la prohibición general del punto 1º.

De los tres que establece, debemos descartar el consentimiento y la ejecución de contrato por motivos a los ya comentadas en la valoración de las bases, quedando la posibilidad de que esté autorizado por el derecho nacional y se den medidas de garantías adecuadas. En relación con esto, podría justificarse en virtud de la Ley de seguridad de las redes y sistemas de información[169], y su artículo 16 al determinar que los prestadores de servicios digitales[170] deberán aplicar las adoptar las medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se

---

utilizado en el videojuego Valorant, que puede extenderse al resto de videojuegos de gran éxito, como son Fornite o League of Legends.

[166] Este tipo de sistemas no se aplican de manera generalizada en la actualidad, pero existen ejemplos de patentes que desglosan todo el flujo de procesos que se llevarían a cabo, como el sistema «*Behavior-aware player selection for multiplayer electronic games*», registrado por Amazon el 20 de octubre de 2020 ante la Oficina Federal de Patentes y Marcas Norteamericana: fig 3 a 6, pág 3 a 6, nº de patente: US 10.807.006 B1.

[167] Se excluye del comentario el interés público y el interés vital por no reunir los requisitos formales para que sean planteables en un escenario hipotético, ya que la organización no estaría ejerciendo una misión conferida por una autoridad pública, ni existe un riesgo para la vida o integridad del interesado o de terceros.

[168] Se ha excluido de la valoración el interés público como posible base para justificar dicha finalidad, teniendo en cuenta que los supuestos reales de dotación a los usuarios de herramientas de grabación y envío de clips de vídeo de la partida o fragmentos de conversación del chat con una presunta infracción de normas de conducta, no respondería realmente a la figura de denuncia interna, y por tanto, con posibilidad de legitimarlo por esta base (*se hace una referencia específica en el apartado V del preámbulo de la LOPDgdd a las denuncias internas se justifican por interés público).*

[169] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[170] La propia ley equipara el concepto de servicio digital al de servicio de la sociedad de la información en su artículo 3.e: *«Servicio digital: servicio de la sociedad de la información*

planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de sus servicios[171].

ii) Información con el objetivo de generar un perfil

Este tipo de profiling, por el contrario, sí que está enfocado en una monitorización más personal para poder modificar ciertos aspectos del juego, reorientar expansiones y contenido postlanzamiento para maximizar el beneficio, y en definitiva, generar métricas, estadísticas y perfiles de jugadores para poder impactarles de manera personalizada.

Los más habituales son la monitorización de la actividad de los jugadores para ver qué contenido es menos popular[172], y la personalización publicitaria (targeting) mostrada en muchas plataformas en función a LA actividad y biblioteca de juegos[173]

En relación con este targeting o segmentación publicitaria, en los casos objeto de estudio se llevan a cabo dos de las tres modalidades principales que enuncia el EDPB en su documento sobre targeting en redes sociales[174], a través de las plataformas de juegos o launchers a los que nos referimos a lo largo del presente estudio:

- Targeting sobre datos observados: sobre todo lo que el jugador hace desde el instante que accede a la plataforma, incluyendo los datos obtenidos por el estudio y editora a través de APIs o kits de desarrollo de software, así como lo que realiza el jugador durante su tiempo de juego efectivo.

- Targeting sobre los datos inferidos: sobre el perfil de jugador que se crea para concluir qué tipo de juegos son lo que se le deben recomendar, o modificar la disposición de la tienda de la plataforma de juego para mostrar primero aquellos considerados de interés. Con la información existente, no es posible conocer si existe una cesión de todos estos tipos de datos entre varios responsables con el objetivo de afinarlo máximo posible, pero en atención a la posibilidad de iniciar sesión en una plataforma con la cuenta de otra, o que en ocasiones se muestran títulos que, o bien se tienen en otras plataformas, o bien se ha consultado en ellas, da un indicativo de que se realiza sin informar adecuadamente[175]

entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico»

[171] El propio considerando 71 apunta a esta idea: *«(…) si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, (…), y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento»*.

[172] Como ejemplos documentados en medios de comunicación sobre este tipo de tratamiento, tenemos los llevado a cabo por el estudio de desarrollo Bioware sobre sus videojuegos de las sagas Mass Effect o Dragon Age para detectar aquellos personajes con los que los jugadores no solían interactuar, y eliminarlos junto con los gastos de desarrollo: líneas de diálogo, animaciones y captura de movimientos, o doblaje, entre otros.

[173] La gran mayoría de plataforma de distribución de videojuegos remiten al jugador ofertas personalizadas basadas en su actividad. Como ejemplo más intensivo, puede destacarse la de la plataforma Steam, que no solo te muestra esta información, sino que en cada juego de la tienda que consultas te muestra una leyenda sobre si ajusta a tus gustos o no.

[174] «Guidelines 8/2020 on the targeting of social media users», de 2 de septiembre de 2020. Este documento está enfocado a desgranar el ecosistema de actores corresponsabilidades y elementos clave dentro del ámbito de las redes sociales, pero contiene elementos aplicables a cualquier tipo de targeting.

[175] Dentro de los muchos de los grandes actores sector existe demanda de data scientist a tiempo completo para gestionar esta faceta tan importante del sector.

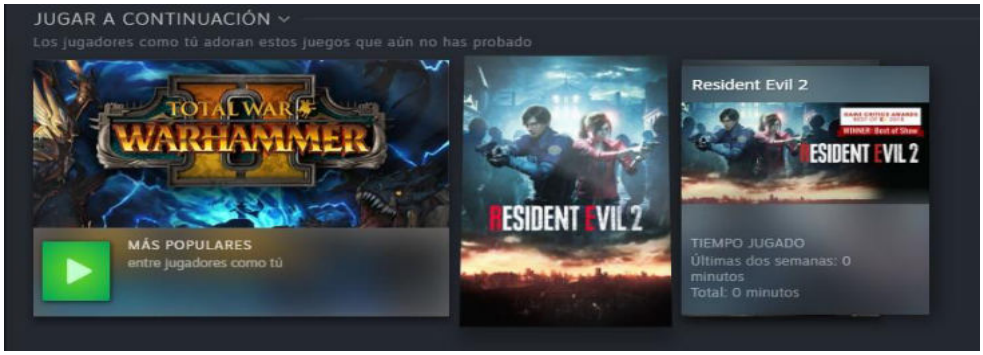
En relación con su posible legitimación, teniendo en cuenta que igual que los anteriores entra totalmente dentro del artículo 22 por estar totalmente automatizado y producir el efecto significativamente similar al jurídico de alterar el comportamiento económico del jugador al ponerle en un lugar principal de la pantalla (*por ejemplo, un pop-up que ocupe la parte central del campo de visión*) aquello a lo que muy difícilmente puede resistirse, solo cabría justificarlo por la vía del consentimiento explícito, junto con el resto de obligaciones y derechos ya comentados que derivan de este artículo.

iii) Información para mejorar la experiencia jugable o ampliarla

Además de los anteriores, se puede hablar de un tercer tipo que trataría datos personales, pudiendo suponer un profiling o no dependiendo del caso, pero cuya principal finalidad es dar una mayor inmersión al juego y no recopilar ningún tipo de información[176].

A diferencia de las anteriores, no tendría por qué estar totalmente automatizado, o ser un profiling como tal. En ese caso, cabría llevarlo por interés legítimo, y si se da en su modalidad totalmente automatiza, consentimiento explícito.

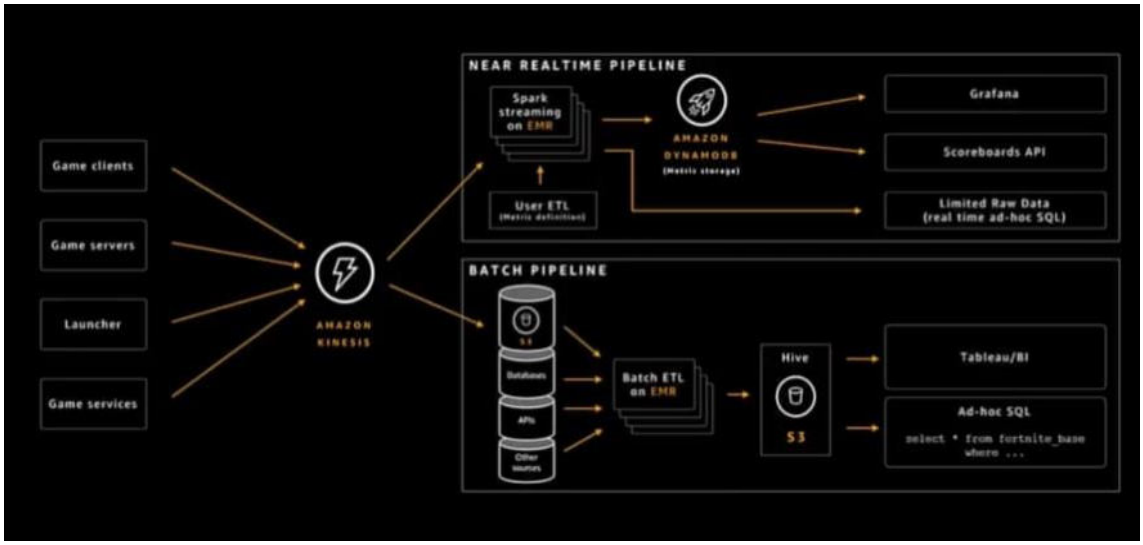
iv) Ejemplos reales de los elementos mencionados en materia de targeting



Ejemplo de mensaje personalizado basado en tu perfil de jugador, que se posiciona en un lugar destacado dentro del campo visual del jugador.

[176] No existen muchos ejemplos de ello, por darse en un género de videojuegos muy inmersivo, pero también de nicho, como es el
ARG o Alternative Reality Game. Dentro de dicha categoría, se encuentra el título The Black Watchmen: a través de una interfaz mínima plantea la narrativa sobre el mundo real con información en páginas web creadas para el juego, lugares, correo electrónico, móvil del jugador, materiales audiovisuales, con el objetivo de ser lo más inmersivo posible y permitiendo al jugador elegir entre varios niveles: correo electrónico, número de teléfono o dirección física para recibir cartas, o incluso actividades en el mundo real.

Ejemplo de información del funcionamiento a grandes rasgos del funcionamiento del sistema de targeting, que no se le da expresamente al jugador, y que solo se encuentra disponible tras un enlace de más información en cada una de las «recomendaciones» personalizadas que se muestran, es decir, después de que el tratamiento se lleve a cabo. Ejemplo de etiqueta (*recuadro menor derecha*) que aparece en aquellos videojuegos en los que el algoritmo determina que no deberían interesarte en atención a tu perfil de jugador.



Ejemplo del flujo de procesamiento de los datos gestionados en el videojuego Fornite por Amazon Kinesis como parte de los serviciosde analítica de datos prestados al responsable del tratamientoi, Epic Games. Fuente: Datanami - Inside Fortnite's Massive Data Analytics Pipeline. Autor: Alex Woodle.

Ejemplo de la información suministrada al jugador en relación al tratamiento de sus datos dentro de las herramientas de chats del responsable por motivo de denuncia por otro jugador. Asimismo, actúa como ejemplo de un consentimiento que no es una clara acción afirmativa que cumpla los parámetros de la actual normativa.

4. Propuestas y recomendaciones

Dentro del enfoque práctico pretendido en el presente estudio, se propondrán una serie de propuestas con el objeto de mejorar o dar solución a ciertas problemáticas concretas que se ha ido abordando a lo largo del documento. Solo se referenciarán aquellas recomendaciones que pudieran suponer una verdadera propuesta de valor para la privacidad y los responsables objeto de estudio, y no las meras indicaciones de cumplimiento de los elementos faltantes en aquellos supuestos que estuvieran cubiertos parcialmente.

4.1. Privacy by design y by default

En atención a garantizar uno de los grandes principios del RGPD y cuyo incumplimiento se categoriza en el artículo 73.d de la LOPDgdd como una infracción muy grave de la normativa[177], se aportan las siguientes propuestas concretas[178]:

4.1.1. Procedimiento de privacy by design y by default

Como forma de garantizar que este principio se cumple[179], así como evitar que ciertos problemas de privacidad o seguridad pasen inadvertidos en el diseño del proceso o servicio que implique un tratamiento de datos personales, se debería establecer un política y procedimiento de privacidad por diseño y por defecto que incluya, al menos, los siguientes elementos:

- Documentación de todas las decisiones y elementos relevantes relacionados con los datos personales como forma de probar ante la AEPD que se cumple con estos principios, así como para tener un control documental.
- Relación de las medidas concretas de privacidad por diseño y por defecto que se apliquen en cada tratamiento que se plantee llevar a cabo.
- Participación del delegado de protección de datos o, en su caso, del responsable de protección de datos de la organización en el proyecto, desde el momento en el que se inicie la planificación del proyecto.
- Obligación de que el delegado de protección de datos o, en su caso, el responsable de protección de datos emita un informa preceptivo en el que determine si el proyecto es adecuado en término de protección de datos.
- Realización de un análisis de los riesgos del proyecto, y en atención al hecho ya citado de que, por el mero volumen de interesados y participación de menores, de una evaluación de impacto.
- Confirmar la implantación de medidas de seudonimización y cifrado por defecto, así como técnicas de anonimización. Especialmente en aquellos tratamientos de mantenimiento de la seguridad que implican el escaneo y análisis de datos de dispositivos personales y no personales.
- Establecer por defecto el uso de protocolos seguros como medida de seguridad en la transmisión de datos personales entre el dispositivo del usuario y el servidor, como los conocidos «https»[180].

[177] Artículo 73.d LOPDgdd.

[178] Se toma como base para realizar dichas propuestas, el tenor literal del artículo 25 del RGPD, y los siguientes documentos específicos sobre esta materia: «Guía de Privacidad desde el Diseño» de la AEPD, «Guía de protección de datos por defecto de la AEPD», «Data protection by design and default» del ICO, y «Directrices 4/2019 sobre el artículo 25 – Portección de datos por diseño y por defecto» del EDPB.

[179] La aplicación efectiva del principio de privacidad por diseño, implica el cumplimiento del resto de principios, al estar intrínsicamente relacionados

[180] LA AEPD en su Resolución de procedimiento sancionador nº 00185/2020, publicada el 10 de noviembre de 2020, sancionada a una determina empresa por, entre otras cosas, no cumplir adecuadamente con el artículo 32 al no disponer de un protocolo de estas características, sino de un inseguro «http».

- Diseñar el uso necesario de patrones y conexiones aplicados a los datos para evitar el uso de API,s, feeds o gateways que pueden poner en riesgo los datos personales.
- Separar los datos personales sensibles o de categoría especial del resto en la base datos, con especial atención a los relativos a menores.
- Exigir la consulta y uso de patrones de privacidad (privacy patterns) para facilitar que el montaje técnico del sistema sea adecuado en materia de privacidad, así como de *Privacy Enhancing Technologies o PETs* [181].
- Implantar salvaguardas y medidas estandarizadas en todos los tratamientos que eviten problemas e imprevistos tras la puesta en marcha del tratamiento. Por ejemplo, eliminar campos innecesarios de los formularios y sistemas de recogida, borrado programado de tablas de indexación entre bases de datos, o separación física y lógica.
- Realizar auditorías periódicas e implantar un proceso de verificación continua que permitan identificar un tratamiento excesivo de datos personales, tratamientos que ya hayan cumplido su finalidad, o modificaciones en los tratamientos que implican una nueva valoración.

4.1.2. Dashboard de privacidad

Con el objetivo de cumplir con este principio y el de transparencia e información, se podría utilizar el área privada de usuario, que ya existe como resultado de ser un servicio que requiere de este tipo de cuenta, para incluir un verdadero panel de privacidad que tenga los siguientes elementos:

- Desactivadas por defecto todas las funcionalidades relacionadas con datos personales y fuentes de datos no autorizados por el usuario debidamente, como, por ejemplo, cesiones de los datos de juego a desarrolladores de los títulos que tenga en la biblioteca, o aquellos que terceros que utilizan herramientas autorizadas de modificación (*modding*) para crear partidas personalizadas, mapas y similares. Asimismo, cumplir con el parámetro de que sea el usuario el que tenga un control real y efectivo sobre sus datos.
- Implementar mecanismos efectivos para ejercer los derechos en materia de protección de datos desde esta área de privacidad. No solo los derechos de acceso y portabilidad, sino la totalidad de los mismos, en atención a que existe la posibilidad técnica de hacerlo y que el usuario ya se encuentra debidamente identificado.
- Agrupar ciertas opciones de configuración, como, por ejemplo, las múltiples modalidades de visibilidad de información del jugador y chats en perfiles predeterminados con distintos niveles para que el jugador pueda elegir el que más que ajuste a lo que quiere. Adicionalmente, se deberá establecer una 2º capa que permita al usuario modificar cada uno de los parámetros en cualquier momento[182].
- Accesible desde la propia plataforma o launcher de juego desde la que el jugador esté accediendo, y no remitirle a la cuenta de usuario vía página web del responsable, ni aplicar ninguna técnica de patrón oscuro o dark pattern.

[181] A este respecto, la AEPD en su documento «Guía de privacidad desde el diseño» incluye varios patrones en su anexo. Asimismo, incluyen referencia a repositorios, como el financiado por la Unión Europa PRIPARE (*Preparing Industry to Privacy by design by supporting its Application in Research*). Asimismo, incluye la referencia a varios repositorios de PETs reconocidos.

[182] Recomendación indicada en la guía de protección de datos por defecto de las AEPD en relación al control del usuario.

- Indexar la información completa de protección de datos en dicho panel para la consulta del usuario en cualquier momento.
- Incluir el panel de configuración de cookies en el mismo, de tal manera que esté a una distancia máxima de dos clicks desde la página de inicio del juego o de la plataforma de juego, y que mediante deslizadores o mecanismos similares permita al jugador marcar y desmarcar las cookies que considere en cada momento[183].

4.2. Información

En atención a dar un cumplimiento adecuado al principio de transparencia y el deber de información de los artículos 12 a 14 del RGPD, se plantean las siguientes propuestas:

- Dividir la información de 1º capa en pantallas sucesivas del proceso de instalación/1º inicio del videojuego que permitan que el usuario sea informado sin generarle fatiga en el proceso, y que además puede generarse una prueba de que efectivamente se le ha cumplido con el mínimo que marca la normativa. En atención al sector en el que se aplicaría, podría redactarse la información con un lenguaje adaptado al mundo de los videojuegos, y con técnicas propia de la gamificación. Por ejemplo, conceder un logro, puntos de jugador o «skins» tras la visualización de todas las pantallas de información, e incluso por visualizar la política de privacidad completa.
- En relación con la anterior, podría valorarse la adopción de información híbrida de texto e iconos, a través de asociar ciertas imágenes o iconos reconocibles por la comunidad de jugadores para cada uno de los apartados de información del artículo 13 y 14, junto con un aviso desplegable en cada uno de ellos con una breve descripción de su significado. Como precedente en el sector de una información mixta de este tipo, está el etiquetado PEGI, ya mencionado en la nota nº 107, por cada uno de los juegos que salen al mercado para indicar visualmente elementos como la edad recomendada, funcionalidades online, presencia de micropagos y loot boxes[184], o la representación de algún tipo de violencia, lenguaje soez, sexo, discriminación o miedo.
- Valorar segregar cierta información específica de las pantallas iniciales de información mediante técnicas de avisos «justo a tiempo o push»[185] para garantizar que el jugador realmente sea consciente de toda ella y evitar la fatiga informativa. Por ejemplo, aplicarlo a la información sobre esos tratamientos de mantenimiento de la seguridad, mayor inmersión, o targeting que implican elaboración de perfiles y decisiones totalmente automatizadas del artículo 22 del RGPD.
- Incluir dentro del menú del juego, preferiblemente con una sección propia o dentro de una etiqueta genérica que deje claro el contenido, como, por ejemplo, «legal»; la política de privacidad específica y la posibilidad de acceso o enlace a los mismos, así como a los derechos en materia de protección de datos.
- En relación con el punto del apartado anterior sobre el panel de privacidad, dar una información clara sobre las distintas funcionalidades en materia de privacidad que se ponen a disposición del jugador a través de sistemas visuales

[183]Incluyendo aquellas librerías de terceros que permitan funcionalidades u otros elementos, La AEPD en su nota técnica de protección del menor en internet destaca como un elemento a informar al usuario.

[184] Paquetes aleatorios de objetos digitales vendidos a un precio fijo, conocidos en español como cajas de botín, y que actualmente están llevando a las autoridades del juego europeas a valorar si constituyen juego regulado o no.

[185] El EDPB (en su momento, Grupo del artículo 29), incluye este tipo de avisos dentro de sus directrices de transparencia como una forma de dividir la información facilitada en fragmentos fáciles de asimilar, y reducir la dependencia de un solo aviso de privacidad.

e informar claramente sobre los metadatos que se tratarán. Por ejemplo, configurarlo para que el 1º acceso al área privada de jugador salte un video explicativo, o que en el 1º acceso se cree una especie de tutorial interactivo que lleve al jugador a pulsar cada pestaña o botón y le indique para qué sirve.

4.3. Menores

En este apartado tan complejo de abordar por el riesgo de que los tratamientos llevados a cabo no vulneren la especial protección e interés superior de la menor reconocida en todo el ordenamiento jurídico, se proponen las siguientes ideas para mejorar dos supuestos concretos de conflicto[186]:

4.3.1. Información al menor

En línea con la idea de la información híbrida de texto e iconos, podría diseñarse una cláusula o sistema informativo con los siguientes parámetros:

- Utilizar un lenguaje adecuado a la edad del menor[187] e intercalar videos explicativos sobre lo que está leyendo y el tratamiento de sus datos que se llevará a cabo[188], con especial incidencia en la horquilla de 13 a 15 años por ser en la que se obtiene plena capacidad para prestar consentimiento en protección de datos, y por cumplir la edad para acceder a juegos que incluyen componentes peligrosos para el menor (*micropagos, juego online, etc*).
- Utilizar mensajes explicativos pop-up que aparezca en el caso de que el menor se plantee modificar alguna funcionalidad que afecte a privacidad desactivada por defecto (*privacy by design*).
- Recordar periódicamente al menor consultar aquella información de privacidad que no hubiera visualizado.
- Establecer información específica sobre los tratamientos del artículo 22 que se pretendan realizar sobre los datos del menor, dejando claro lo que se pretende hacer y sus consecuencias. Sería recomendable establecer un código de colores de verde y rojo para que visualmente quede claro desde un inicio.
- «Children approach by defect»: en el supuesto en el que no sea posible realizar dos versiones distintas de la información para menores y adultos, optar por la específica para menores a fin de poder cumplir con ambos espectros de responsabilidad.
- Evitar utilizar técnicas o sistemas que induzcan al menor a aceptar o pulsar cualquier botón, aun cuando, no se le diga nada en este sentido[189]

[186] Se excluye el comentario sobre técnicas de control parental debido a que existe un cumplimiento adecuado en las organizaciones objeto de estudio. Particularmente, en el ámbito de las consolas por ser el sistema de juego usado en gran medida por menores, ya sea en sus modalidades portátiles o de sobremesa.

[187] El ICO en su documento: «Age appropriate design: a code of practice for online services», incluye recomendaciones concretas de cómo facilitar la información a menores según el grupo de edad en el que se encuentren: 0-5, 6-9, 10-12. 13-15, y 16-17.

[188] El ICO en su documento de buenas prácticas en servicios digitales para menores recomienda la utilización de vídeos y de elementos netamente visuales para conseguir captar mejor la atención del menor y que entienda sin género de dudas la información que se le muestra.

[189] Como las técnicas conocidas como «nudge techniques», consistentes en hacer más atractiva la opción que se quiere que marce el usuario, mediante un texto más bonito, un color más impactante, un botón más grande, o una localización que se sabe que se pulsa instintivamente, entre otros ejemplos.

4.3.2. Comprobación de edad del menor

En aquellos casos en los que es necesario determinar la edad del jugador, se utilizan los sistemas ya comentados de la mera indicación de la edad o una casilla específica para que el menor marque y active el sistema para su tutor o padre hagan una cuenta principal, que no arrojarían una prueba real y válida en los términos del RGPD para que el responsable pueda demostrar que ha tenido una diligencia adecuada y proporcional a su capacidad para determinar si el menor tenía 14 años o no.

Teniendo en cuenta estas dos modalidades utilizadas comúnmente, y, también, que el interés superior del menor y la protección reforzada que el RGPD incluye en su articulado impediría cualquier intento de comprobación de la veracidad del documento de identidad por reconocimiento facial y otros sistemas que perfilen al menor para decidir automáticamente si por su navegación lo es o no, y que por el volumen a interesados a tratar implicaría que fuera totalmente automatizado; se plantean dos opciones para llevarlo a cabo:

i) Comprobación automatizada de edad por cotejo de fechas

Habilitar un sistema en base a los siguientes parámetros, ordenados en función a las distintas fases del proceso:

- Solicitud de introducción de una fecha a través del sistema de campos a este efecto, con un aviso de que se revise que los datos introducidos son correctos.
- Solicitud de una imagen del anverso del documento nacional de identidad en el que figura la fecha de nacimiento, eliminando en el proceso cualquier otro dato que no sea dicha fecha de nacimiento o el nombre y apellidos para que nunca lleguen a ser almacenados, especialmente la fotografía. Podría valorarse permitirle al jugador visualizar previamente cómo quedaría su imagen de DNI tras ese proceso de eliminación automática de los datos distintos de la fecha de nacimiento y el nombre y apellidos.
- Cotejo totalmente automatizado de la coincidencia de fechas para seguir con el proceso de creación de la cuenta, o, caso de resultar negativa, el bloqueo con registro de la IP desde la que se accede para exigir en posteriores intentos la apertura de una cuenta principal por el tutor o progenitor que autorice continuar con el proceso.

Esta solución planteada implicaría una decisión totalmente automatizada que produce efectos significativamente similares a los jurídicos en el menor, pero limitada al cotejo de fechas y con la garantía específica de la eliminación automática del resto de datos por no ser posible no recabarlos de una imagen. Asimismo, le permitiría al responsable generar una prueba real frente a terceros y la propia AEPD de que se ha implantado un sistema razonable, no desproporcionado y adecuado a su mayor capacidad técnica, organizativa y de medios para lograr la finalidad buscada.

ii) Comprobación a través del DNIe

Alternativamente, existiría la posibilidad de identificar de comprobar la edad a través del certificado de autenticación del DNI electrónico que se activa automática en su expedición a menores, sin que incluya ninguna funcionalidad de firma electrónica solo sirva a los efectos de identificarlo inequívocamente [190], de conformidad al artículo 1.4, segundo párrafo de la ley de expedición del DNI y sus certificados electrónicos[191].

[190] La propia Agencia Española de Protección de Datos proponía esta modalidad como vía para lograr esta identificación del menor en el ámbito digital, y el legislador lo incluyó finalmente en el año 2013 dentro de la ley reguladora del documento nacional de identidad y sus certificados.
[191] Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

Este sistema implicaría que el menor tuviera acceso a un lector de tarjetas inteligentes compatible con la versión de DNI-e que posea.

4.4. Certificaciones y códigos de conducta

En aplicación del artículo 40 del RGPD y del principio de responsabilidad proactiva, se propone la creación de los siguientes códigos de conducta, que posteriormente sean remitidos a la AEPD para su aprobación definitiva.

4.4.1. Código de desarrollo para responsable del tratamiento

Para garantizar un estándar de protección de datos a nivel de la industria se plantea la creación de un código de conducta a nivel español o europeo, vehiculado a través de las asociaciones representativas de los responsables en cada caso: España (*AEVI o DEV*), y Europa (*ISFE o EGDF*). Dentro de que el contenido se enfoque en adecuar cada apartado del RGPD aplicable al sector de los videojuegos[192], debería contener referencias específicas a lo siguiente:

- Tratamientos de protección de datos específicos del sector de los videojuegos y sus garantías para llevarlos a cabo, de conformidad a la normativa.
- Desarrollo de los distintos casos de corresponsabilidad que existen en el sector.
- Procedimiento a seguir en el diseño de tratamiento para cumplir el principio de privacy by design.
- Formas adecuadas y recomendable de mostrar la información a los jugadores, especialmente a los menores.
- Relación de patrones de privacidad aplicables al desarrollo de un videojuego para garantizar la aplicación de los principios de privacy by design y by default.
- Transferencia internacional de datos a países fuera de espacio económico europeo y de los estados con decisiones de adecuación, especialmente a Estados Unidos, a efectos de dotarlos de los elementos necesarios para poder servir como garantía que permita transferirlos en la nueva realidad posterior a la derogación del acuerdo privacy shield[193], teniendo en cuenta el riesgo mencionado de control federal por seguridad nacional.

4.4.2. Código de conducta de encargados

A fin de generar una prueba que permita probar al responsable que ha sido diligente en la elección del encargado del tratamiento adecuado, se propone, al igual en el caso anterior, la creación de un código de conducta específico que contenga los elementos necesarios, siguiendo las pautas del artículo 28, pero añadiendo los elementos que contiene el código de conducta de la asociación NLDIGITAL, ya citado:

- Obligación del encargado de entregar al responsable una declaración de cumplimiento del código como parte del proceso de selección del encargado.
- Obligación del encargado de mantener una política propia de privacidad adecuada y actualizada.

4.4.3. Marca de privacidad en el etiquetado

Siguiendo lo dispuesto en el artículo 42 del RGPD, el principio de transparencia y la autorregulación del sector de los videojuegos tendente a etiquetar cada uno de los sale al mercado con información clave de su contenido, se plantea la creación de una marca

[192] Como punto de partida podría utilizarse lo ya recogido en la guía de RGPD para desarrolladores de la CNIL.
[193]De conformidad al artículo 64.1.b del RGPD, se requiere adicionalmente que el EDPB emita un dictamen al respecto.

o símbolo que identifique que el responsable cumple con la normativa en materia de privacidad, con los siguientes parámetros:

- La marca sea integrada dentro del sistema de etiquetado de videojuegos europeos PEGI para dar mayor confianza al jugador y hacerlo de manera homogénea a nivel de toda la Unión Europea.
- Sea concedida tras un proceso de valoración o certificación de cumplimiento, con un límite de vigencia y auditorías periódicas de renovación y control.
- Sea parte de las obligaciones del responsable recogidas en el código de conducta propuesto.

4.5. Sistema de denuncias (whistleblowing) adaptado

En atención a que el tratamiento de prevención de trampas es tan importante para mantener el servicio prestado en condiciones adecuadas, así como para garantizar un adecuado tratamiento de los datos de denunciante y denunciado, se propone establecer un procedimiento propio inspirado en el relativo a denuncias internas o whistleblowing y su normativa[194], con los siguientes parámetros:

- Obligación del denunciante de utilizar un seudónimo distinto al que tiene como nombre de jugador (*el responsable conocerá el ID real al ser el asociado a la cuenta de usuario desde la que se tramita la denuncia*), con el objetivo de que no pueda ser identificado por el denunciado a través de la comprobación de mensaje internos de chat en el momento en el que ocurría la conducta denunciada, o por cualquier otra vía distinta
- Generación de acuse de recibo para el denunciante en el momento de presentación de la denuncia.
- Garantizar que el denunciante lo haga de manera voluntaria, sin que en ningún momento se le obligue contractualmente o de cualquier otro modo. Por un lado, estaría esta voluntariedad que no debería entenderse como consentimiento en materia de protección, y por otro, la base de legitimación que justificaría el tratamiento de datos por parte del responsable.
- Minimizar los datos a lo estrictamente necesario: ID del denunciante, ID del denunciado, y prueba de la posible infracción o conducta prohibida.
- Comunicación al denunciado para que pueda comunicar lo que se considere oportuno, así como cualquier elemento de prueba a su favor.
- Establecimiento de plazos máximos de tramitación y resolución de las denuncias[195].
- Mantenimiento de un registro de todas las denuncias tramitadas, tanto de las desestimadas, como de las estimadas.

4.6. Limitación del alcance de los sistemas antitrampas

En atención a que los sistemas de escaneo y monitorización del jugador con el objetivo de prevenir el fraude y la comisión de trampas en el juego ya comentados puedan ser legales, debería plantearse una serie de elementos que conformen unas garantías mínimas con las que poder superar una evaluación de impacto:

[194] Lo recogido en el artículo 24 de la LOPDgdd, y en la Directiva 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones.

[195] En atención a la naturaleza, complejidad, automatización y efectos de los hechos denunciados, el plazo de 3 meses marcado como límite por la LOPDgdd para mantener los datos en el sistema sería excesivo.

- Limitación del tiempo de monitorización a la sesión de juego[196], y de su alcance a la actividad del jugador durante ese tiempo y a los archivos del videojuego dentro de sus carpetas de instalación. En ningún caso, ese control debería aplicarse al resto de programas y archivos del ordenador, tal y como hacen en la actualidad los sistemas utilizados por los principales actores del sector.
- Información previa y clara antes de la activación del sistema, de manera que el jugador sepa que desde ese momento lo que haga será monitorizado de manera totalmente automatizada para determinar si utiliza algún tipo de programa o conductas prohibidas. Específicamente, se le deberá informar de la lógica del algoritmo y sus consecuencias, el derecho a intervención humana y a opinar e impugnar de la decisión.
- Aviso o ventana emergente visible para el jugador que indique el inicio y el fin de la monitorización en cada una de las sesiones. En el caso de que el jugador no cierre la sesión, debería configurarse de manera que se detenga dicha monitorización y dé aviso igualmente al usuario al detectar que no hay actividad.
- Recomendable publicar una versión muy resumida y visual de los elementos clave de la evaluación de impacto realizada, especialmente, de las garantías aplicadas para asegurar los derechos del jugador en el tratamiento, como una forma más de transparencia y responsabilidad proactiva del responsable.
- Legitimarlo por la vía ya comentada del interés legítimo junto con la excepción del artículo 22 del RGPD de estar autorizado por norma nacional (*Ley de seguridad de las redes y sistemas de información*). En el caso de perfilado para segmentación publicitaria, como ya se han mencionado, solo cabría la vía del consentimiento explícito.

4.7. Loot boxes o cajas de botín

Tanto en el supuesto en el que suponga un tratamiento de datos personales o no como se ha indicado, se plantean las siguientes propuestas a fin de minimizar el riesgo de discriminación del algoritmo que lo sustenta:

- Incluir una llamada visual que despliegue una pantalla con los porcentajes actualizados que tiene cada objeto de salir en cada caja de botín, a fin de informar al jugador de una manera más orgánica de la lógica y condiciones que utiliza el algoritmo.
- Garantizar una información adecuada, especialmente pensando en menores. En el caso de que suponga un tratamiento de datos al asociarlo al perfil de jugador y se conozca que es un menor, limitar el número de cajas de botín que puede adquirir desde dicha cuenta.

[196] Actualmente, al igual que las redes sociales y la gran mayoría de servicios digitales, es necesario autenticarse con tu cuenta de usuario antes de poder entrar a jugar cada vez que se acceda o habilitando la opción de recordar sesión.

5. Consideraciones finales

Como se ha indicado en la introducción, la industria de los videojuegos es un sector de gran popularidad y con una facturación que se incrementa exponencialmente por ser una de las formas de entretenimiento hegemónicas, siendo en grandes términos internacionales uno de los sectores que ha conseguido resistir en la gran pandemia que nos asolado y que sigue desplegando efectos nocivos sobre todos nosotros, junto con las grandes tecnológicas con las que comparten campo de juego.

A diferencia de otros sectores de gran arraigo sobre los que el legislador ha puesto el foco para garantizar las reglas del juego, la joven industria de los videojuegos (*data de los años 70*) ha sido un gigante invisible que ha ido rompiendo récords de crecimiento y facturación sin que se viera la necesidad de regular específicamente a este nuevo jugador, o tratar la gran complejidad y afectación para el entorno jurídico de los jugadores que supone la necesidad de tratar datos de todo tipo en tiempo real para que algo de esa magnitud funcione correctamente.

A pesar de que de la lectura del presente estudio pudiera concluirse que la industria de los videojuegos tiene un cumplimiento en materia de protección de datos al nivel de otros sectores, con sus luces y sombras, lo cierto es que fuera de los grandes actores analizados, no existe un cumplimiento generalizado ni el conocimiento de que sea algo obligatorio y necesario per se. Como el resto de sectores, el mayor porcentaje del mismo lo componen pequeños actores (*conocidos como indies*) que no tienen ese nivel de recursos y capacidad para destinarlos a tener un departamento legal y valorar qué ámbitos legales deben cumplir más allá de que su videojuego llegue al mercado.

Sin ánimo de repetir nada de los expuesto o argumentado en el estudio, puede concluirse que gran parte de los tratamientos que generan dudas o problemas, podrían llevarse a cabo si se modifican ciertos parámetros para permitir que la evaluación de impacto sea positiva. En un sector que necesita un tratamiento de datos tal alto, está intrínsicamente condenado a entenderse con la privacidad de una manera muy estrecha.

En un sector con una incidencia tan grande de menores de edad, deberían implementarse sistemas de comprobación de edad, y de información adecuada que estuvieran a la vanguardia del entorno digital por ese mayor riesgo existente. Debe realizarse una gran labor de concienciación con los jugadores por parte de los responsables, no solo porque pudiera servir como prueba para demostrar responsabilidad proactiva, sino porque los propios jugadores, en general, no son conscientes de la importancia de su derecho fundamental a la protección de datos, o anteponen el poder mantener una partida entre varios dispositivos a consentir informadamente ciertos parámetros para ello.

Finalmente, esa mayor presencia de los grandes tecnológicas para posicionarse en este lucrativo negocio, puede ser una buena oportunidad para que las autoridades de protección de datos pongan el foco en este sector y se propongan directrices y guías que analicen y mejoren la protección de datos en el mismo

6. Bibliografía

1) Copia digital de la documentación objeto de estudio

1. Enlace al repositorio en nube: https://drive.google.com/drive/folders/1dzzqvMjpBsubEbFq1J9K8nAe4qnjprBU

2) Documentos de autoridades de protección de datos y europeas

Autoridad federal alemana de protección de datos alemana (BFDI)

2. Documento de posición para la anonimización bajo el RGPD con especial consideración del sector de las telecomunicaciones, de 26 de junio de 2020 https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2

Autoridad de protección de datos británica (ICO)

1. «Guide to the General Data Protection Regulation (GDPR)»: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
2. «Guidance on the use of cookies and similar technologies». https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/
3. «Age appropriate design: a code of practice for online services», de agosto de 2020. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

Autoridad de protección de datos francesa (CNIL)

1. «Guía para desarrolladores», de junio de 2020. https://www.cnil.fr/en/gdpr-developers-guide

Agencia española de Protección de Datos (AEPD)

1. «Guía para el cumplimiento del deber de informar», mayo de 2018 (realizada conjuntamente con las autoridades catalana y vasca) https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf
2. «Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos», de 16 de mayo de 2019: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf
3. «Estudio de Fingerprinting o Huella digital del dispositivo», febrero de 2019. https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf
4. «Guía de protección de datos por defecto», de octubre de 2020. https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf
5. «Guía de privacidad desde el diseño», de octubre de 2019. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf
6. Informe 0036/2020, de 8 de mayo de 2020. https://www.aepd.es/es/documento/2020-0036.pdf

7. «Guía sobre el uso de las cookies, de julio de 2020». https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

Autoridad catalana de protección de datos (APDCAT)

1. Dictamen 21/2020, de 12 de junio de 2020. https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-21-2020-00001

Comité Europeo de Protección de datos (EDPB)

1. «Dictamen 5/2009 sobre las redes sociales en línea del Grupo del artículo 29», de 12 de junio de 2009. https://www.apda.ad/sites/default/files/2018-10/wp163_es.pdf
2. «Directrices sobre los delegados de protección de datos (DPD)», de 5 de abril de 2017. https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guidelines-on-Data-Protection-Officers.pdf
3. «Directrices sobre transparencia en virtud del Reglamento (UE) 2016/679», de 11 de abril de 2018 https://apdcat.gencat.cat/web/.content/03 documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf
4. «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», de 6 de febrero de 2018 https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp251rev01_es-decisions-automatitzades.pdf
5. «Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679, de 25 de mayo 2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf
6. «Directrices 1/2019 sobre códigos de conducta y autoridades de supervisión y control en virtud del Reglamento 2016/679», de 12 de febrero de 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf
7. «Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del Reglamento (UE) 2016/679 en el contexto de la prestación de servicios en línea a los interesados» de 8 de octubre de 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf
8. «Directrices 05/2020 sobre el consentimiento en virtud del Reglamento (UE) 2016/679» , de 4 de mayo de 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
9. Cláusulas tipo para contratos de encargados de tratamiento de la autoridad danesa, validadas por el edpb, de enero de 2020 https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf
10. «Directrices 1/2018 sobre la certificación y la identificación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento (UE) 2016/679», de 4 de junio de 2019. *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf*
11. «Directrices 8/2020 sobre segmentación de usuarios de redes sociales», de 2 de septiembre de 2020.

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf
12. «Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE», de 11 de noviembre de 2020 (*consulta pública*). https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Supervisor Europeo (EDPS)

1. «Estrategia para las instituciones, dependencias, organismos y agencias de la unión en el cumplimiento de las reglas: Schrems II» de 29 de octubre de 2020. https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf
2. «Directrices sobre los conceptos de responsable, encargado y corresponsable en virtud del Reglamento (UE) 1725/2018», de 7 de noviembre de 2019. https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

Comisión europea (CE)

1. «Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea», de 9 mayo de 2019: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019DC0250&from=en
2. «Borrador de propuesta sobre las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679», de 12 de noviembre de 2020 (*el texto de la cláusula figura en el anexo*) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

Consejo Europeo

1. «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas y por el que se deroga las Directiva 2002/58/CE», versión de 8 de noviembre de 2019. https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf»

3) Autoridades federales norteamericanas

1. «Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II». *https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF*
2. Patente US 10.807.006 B1 «Behavior-aware player selection for multiplayer electronic games» de Amazon, fig 3 a 6, pág 3 a 6. https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=10807006&IDKey=DF8030302054%0D%0A&HomeUrl=http%3A%2F%2Fpatft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO2%2526Sect2%3DHITOFF%2526u%3D%25252Fnetahtml%25252FPTO%25252Fsearch-adv.htm%2526r%3D97%2526f%3DG%2526l%3D50%2526d%3DPTXT%2526s

1%3Damazon.ASNM.%2526p%3D2%2526OS%3DAN%2Famazon%2526RS%3DAN%2Famazon

4) Documentos del sector de los videojuegos utilizados

1. Asociación española de empresas desarrolladoras de videojuegos y software de entretenimiento: «Libro blanco del desarrollo español de videojuegos 2019»: https://www.dev.org.es/images/stories/docs/libro%20blanco%20dev%202019.pdf
2. Asociación española de videojuegos, 2019 – « *La industria del videojuego en España – Anuario 2019*»: http://www.aevi.org.es/web/wp-content/uploads/2020/04/AEVI-ANUARIO-2019.pdf
3. Federación Europea de Software Interactivo (ISFE), 2019 – « *Proposal for an e-Privacy Regulation Recommendations for the Finnish Presidency».* https://www.isfe.eu/wp-content/uploads/2018/04/ISFE-position-paper-on-ePR-Recommendations-for-the-Finnish-Presidency.pdf
4. Federación Europea de Software Interactivo (ISFE), 2019- « In-Game Spending Study GameTrack Nov 2019». https://www.isfe.eu/wp-content/uploads/2019/12/GameTrack-In-Game-Spending-2019.pdf
5. Consultora Newzoo: *« Newzoo Global Games Market Report 2020»*: https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2020-light-version/

5) Normativa utilizada

1. Reglamento 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
2. Reglamento (UE) 2018/1807, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, de 14 de noviembre de 2018.
3. Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.
4. Reglamento (ue) 2019/1150 del parlamento europeo y del consejo de 20 de junio de 2019 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea
5. Ley Orgánica 1/1996, de Protección Jurídica del Menor, de 15 de enero.
6. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
7. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
8. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
9. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

6) Resoluciones

1. Sentencia 27/2020 del Tribunal Constitucional: https://hj.tribunalconstitucional.es/es/Resolucion/Show/26246
2. Resolución del Tribunal de Justicia de la Unión Europea «C-25/17 Jehovan todistajat».

http://curia.europa.eu/juris/document/document.jsf;jsessionid=40B820DE046CE7104025ABC633CB6021?text=&docid=203822&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10661541
3. Resolución del Tribunal de Justicia de la Unión Europea «C-40/17 Fashion ID». http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10661591
4. Resolución del Tribunal de Justicia de la Unión Europea «C-210/16 Wirtschaftsakademie Schleswig-Holstein». http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10661833
5. Resolución del Tribunal de Justicia de la Unión Europea «C-673/17 Planet 49». http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=11550415

7) Artículos y fuentes doctrinales

1. ALEX BOUTILIER. «Video game companies are collecting massive amounts of data about you» diciembre de 2015. https://www.thestar.com/news/canada/2015/12/29/how-much-data-are-video-games-collecting-about-you.html
2. ALEX WOODIE. «Inside Fortnite's Massive Data Analytics Pipeline», julio de 2018. https://www.datanami.com/2018/07/31/inside-fortnites-massive-data-analytics-pipeline/
3. LOGAN ERICKSON. «Big Data Gaming: The Practice and Use of Big Data at Electronic Arts», noviembre de 2016. http://cdn.law.utah.edu/praxis/papers/Erickson.pdf
4. STEVEN BLICKENSDERFER y NICHOLAS A. BROWN. «Even the Games Have Eyes: Data Privacy and Gaming», marzo de 2019. https://www.natlawreview.com/article/even-games-have-eyes-data-privacy-and-gaming-podcast
5. OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. «Gaming and personal information: playing with privacy», mayo de 2019. https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/gd_gc_201905/
6. PATRICK STAFFORD. «The dangers of in-game data collection: Can your choices come back to haunt you?», mayo de 2019. https://www.polygon.com/features/2019/5/9/18522937/video-game-privacy-player-data-collection