Premio de Investigación en Protección de Datos Personales Emilio Aced 2024

Análisis de la adecuación y funcionamiento de los sistemas antitrampas o «*anti-cheat*» en los videojuegos. Comentario especial del escaneo en tiempo real y a nivel de administrador del dispositivo de juego.

Autor: Darío López Rincón

20 de septiembre de 2024

Índice de contenido

Índice de figuras

1. Introducción y planteamiento general del estudio

1.1. Contexto

La industria de los videojuegos es un sector que desde sus inicios ha intentado implementar medidas que le permitan defender su propiedad intelectual, la seguridad de sus sistemas, prevenir que los jugadores puedan alterar la partida, jugar a copias ilegales o cualquier conducta contraria a la ley y a los términos y condiciones establecidos.

Para intentar lograrlo, además de la eventual obligación y repercusiones legales (*sanciones e imposibilidad de acceso*) que suponen la aceptación como usuario final del contrato o «EULA»[1], se ha confiado en medidas de protección tecnológica[2] en una doble modalidad:

- Sistemas de «*Digital Rights Management*» o «*DRM*», por sus siglas en inglés, que controlan el acceso legítimo a una copia legal del videojuego o la imposibilidad de copiarlo, es decir, lo que se suele conocer como «piratería»[3]; y

- Sistemas «*anti-cheats*» o antitrampa, objeto del presente estudio, para analizar y parametrizar en tiempo real lo que el jugador realiza dentro y fuera de partida que pudiera afectarla.

En los primeros compases de la industria de los videojuegos que no permitían un juego multijugador en línea en sentido estricto[4], se implementaron medidas de control puro del primer tipo comentado de DRM. En particular, dichas medidas se desplegaban en dos ámbitos:

- **Físicas:** en cada caja o carcasa se incluía algún medio de seguridad física que se requería que el jugador pudiera probarlo para validar la copia del juego al que pretendía jugar por primera vez. Entre multitud de ejemplos, cabe destacar el caso de las claves impresas de único uso, sistemas más elaborados de diales de cartón rotatorios con varias configuraciones y distintos números por cada uno, o la necesidad del uso de lentes especiales para leer un código en pantalla que sin ellas parecería ininteligible.[5]; y

- **Tecnológicas:** a nivel de programación, los desarrollares configuraban una determinada respuesta del videojuego ante la detección de una copia falsa, alteraciones en hardware o la imposibilidad de activar el juego con la clave o control exigido. Como ejemplos más característicos y conocidos en este sentido, tendríamos la modificación del canto gregoriano del videojuego español «*La abadía del crimen*» por otro en el que solo repetían la palabra «*pirata*», la

[1] El acrónimo resultante de la denominación completa del tipo de contrato en inglés: «*End-user License Agreement*», utilizadas como denominativo en el argot de la industria.

[2] Aunque responde a un concepto exacto y con significado propio de la normativa de propiedad intelectual, se utiliza en el presente caso como una expresión general sobre medidas con componente tecnológico para prevenir conductas y actos no permitidos.

[3] A nivel de jugador y consumidor general, son dos conceptos que se utilizan como sinónimos por la propia confusión y funcionalidades cruzadas que da un sistema de control, pero se considera relevante establecer esta diferencia terminológica y de fondo clave a nivel de la intromisión en materia de protección de datos.

[4] Sí permitían un juego en línea limitado a la propia consola, o conectando varias consolas entre sí denominado «*juego en local*». Generalmente, es conocido por implicar la división de la misma pantalla de juego en partes y proporción iguales para cada jugador.

[5] Como ejemplos reales de lo comentado: el dial de cartón llamada «*Dial-A-Pirate*» que el videojuego de aventura gráfica, «*Monkey Island*», incluía en cada caja de copia del juego; o la lente «*Lenslok*» que permitía leer código correctamente que aparecía en pantalla.

imposibilidad de planeo del personaje o la ralentización excesiva que impedía completar el juego en Batman Arkham Asylum y Mirror's Edge, respectivamente.

Con la consolidación del juego online, la copia digital, la exigencia de conexión permanente a internet y el modo de juego multijugador; surgió la necesidad de complementar esos primeros sistemas con los segundos antitrampas, enfocados en controlar si el jugador realizar alguna conducta prohibida.

La actualidad existente de permitir el juego sólo a través «*clientes de juego*» o «*launchers*»[6], facilita en gran medida el funcionamiento de cualquier sistema que se configure para actuar o transmitir información a su través, así como la aplicación automática de cualquier sanción al jugador infractor: desde una limitación de acceso temporal, hasta una total con la perdida de toda la biblioteca de juegos adquiridos en el determinado cliente de juego.

A nivel doctrinal y académico, especialmente desde la investigación de la cuestión por su vertiente más conceptual y de análisis de la figura, existen multitud de definiciones de trampas, o del hecho de hacerlas (*más conocida esta práctica en su terminología original inglesa: «cheating»*.) Se considera de mayor relevancia por comprender todos los elementos característicos de esta materia, las siguientes conceptualizaciones[7]:

- «*Cualquier comportamiento que un jugador pueda utilizar para obtener una ventaja injusta, o alcanzar un objetivo que se supone que no debe, es trampa*». Jeff Yan & Choi, 2002);

- «*Hacer trampas se considera generalmente como modificar la experiencia de juego de alguna manera con el fin de obtener una ventaja sobre los demás jugadores para obtener una ventaja sobre los demás jugadores*». (Chen et al., 2005);

- «*En general, estas definiciones pueden resumirse en 3 partes: 1) hacer trampas implica explotar las lagunas en los sistemas de juego, 2) tales comportamientos conducen a ventajas injustas sobre otros jugadores, 3) estas ventajas son injustas porque no se supone que los jugadores conseguirse de acuerdo con las reglas del juego o los códigos de conducta*». (Duh & Chen, 2009); o

- «*En general, "hacer trampas" es cuando un jugador toma el control de la experiencia de juego utilizando recursos ajenos a uno mismo en lugar de jugar según las reglas*». «*En el modo multijugador, siempre que un jugador emplea una táctica que da ventaja en sobre los demás o que altere el formato de juego previsto, existe un consenso general de que se trata de una forma inaceptable de hacer trampas*». (Doherty et al., 2014).

A efectos del presente estudio, se podría asumir cualquier de las cuatro definiciones presentadas. No obstante, se considera relevante incluir dos elementos adicionales que, actualmente, forman parte del ecosistema de prevención de actuaciones contrarias del jugador, sean trampas en el juego u otras conductas no permitidas. Se tratarán de manera separada en los apartados 2.3 y 2.4 del presente estudio, por el elemento de no aplicarse al dispositivo del jugador, sino sólo a las herramientas de comunicación y las

[6] En el caso de juego de consola, sea portátil o no, no existe un denominativo específico al ser un dispositivo con una configuración cerrada y que permite exclusivamente el juego y la reproducción de contenido en formato de disco, en su caso.

[7] Extraídas de la selección realizada por el autor, Heikki Haapaniemi, en su estudio «*Cheat detection & prevention methods in video games*». Universidad de Oulu, Tabla 1, «Appendix A. Table 1. Definition of cheating», pág. 32.

dadas para que otros jugadores comuniquen posibles trampas visualizadas, Es decir, acotado su efecto a la plataforma o cliente de juego que corresponda en cada caso:

- La alternativa de que otros jugadores puedan «*denunciar*» a presuntos infractores, mediante las funcionalidades que ofrece el videojuego dentro y fuera de la partida, la indicación del nombre de usuario para que se revise su perfil, partidas u otros elementos. Muy similar a cualquier sistema de denuncia de cualquier red social o plataforma digital actual dispone a efectos similares.; y

- La grabación, análisis y moderación de los distintos «*chats*» y canales de comunicación por voz que el juego permita, a fin de detectar y cortar de manera remota acceso por lenguaje inapropiado o conductas prohibidas en el «*código de conducta*» o «*reglas de la comunidad*»[8] aplicables.

Centrando la cuestión sobre los sistemas antitrampas objeto de estudio, existen múltiples formas técnicas de configurar un sistema de prevención de este tipo, pero en la actualidad se utilizada manera hegemónica el acceso a nivel de administrador, o también llamado «*Kernel*» o «*acceso a nivel O*». Este tipo de acceso total y obligatorio al dispositivo del jugador en todo momento que se realiza de manera estandarizada, habitual y asumido por necesidad por los jugadores, implica la asunción de una serie de riesgos de seguridad, frente a ataques maliciosos y, sobre todo a nivel del derecho fundamental a la protección de datos.

Unos sistemas que se van actualizando conforme la tecnología permite un mayor grado de automatización y reducción de costes: machine learning, inteligencia artificial[9], diversos prototipos o funcionalidades sobre seguimiento ocular o sensores de bioseñales en visores de realidad virtual, a nivel de patente o no comercializadas al gran público actualmente[10]; o el previsible futuro a medio plazo de funcionalidades a nivel neural y con su afectación a los «neuroderechos»[11].

Asimismo, dichos sistemas se encuentran envueltos en polémica a nivel de prensa especializada, por tres razones principales:

- Que su efectividad real se percibe como baja por poder arrojar falsos positivos que provocan bloqueos automáticos de jugadores legítimos, o implicar una serie de perjuicios tangibles para todo jugador a nivel de rendimiento del ordenador, rendimiento del juego, obligación de conexión permanente a internet, obligación de desactivación de determinados programas legítimos, antivirus o excepciones a cortafuegos y seguridad;

[8] Documento con efecto legal en el que se detalla, de manera sucinta y en lenguaje coloquial, que el jugador no deberá utilizar trampas, lenguaje malsonante, cualquier fallo del juego, subir contenido apropiado si se dan herramientas para ello, usurpar la identidad de otros jugadores, o que todas estas conductas llevarán aparejado un bloqueo. En algunos supuestos, se detallan las posibles sanciones, estratificadas o con sus respectivos criterios de valoración.

[9] NVIDIA, uno de los principales fabricantes de tarjetas gráficas y de computación de alto rendimiento, junto con un investigador de la Universidad de California, desarrollan en un estudio el posible uso de sistemas de red neuronal para poder detectar cambios en los fotogramas de la imagen que arrojen indicio de comisión de trampas. d– «*Robust Vision-Based Cheat Detection in Competitive Gaming*»

[10] Por ejemplo, la patente de Meta con numeración y denominación: US20170352183 – FACE AND EYE TRACKING USING FACIAL SENSORS WITHIN A HEAD-MOUNTED.

[11] A pesar de ser una materia de notable desarrollo y avance, se considera que el marco de aplicación temporal estaría más a medio plazo por el hecho de no existir actualmente sistemas que se prevea comercializar en breve. En el apartado 2.7 se realizará un breve comentario al respecto.

- Que dichos sistemas, con independencia del nivel de robustez presumido por su proveedor, son objeto de superación por grupos de piratas informáticos o fabricantes y comercializadores de software de trampas; y por

- El hecho de que el control sobre el jugador se intensifica cada vez más para intentar evitar la piratería mencionada, así como la progresiva toxificación social en internet. Como ejemplo más polémico al respecto, las funcionalidades más recientes de grabación de la voz de cualquier chat o sistema de comunicación interno del juego para prevenir cualquier insulto, discurso de odio o acoso.

1.2. Objeto y alcance

El objetivo de este estudio es analizar, desde el punto de vista de protección de datos y del propio interesado, el tratamiento que implican este tipo de sistemas antitrampas a nivel de kernel o administrador. A efectos de concreción, este tratamiento se divide en cuatro fases principales:

- Análisis del dispositivo y de sus archivos, programas e información para detectar cualquier cambio o indicativo de instalación de algún elemento que pudiera ser considerado una trampa, programa que lo permitiera o elemento en conflicto con el sistema antitrampa. En tiempo real, pero iniciándose en el encendido del dispositivo para cualquier fin, o desde el proceso de apertura y carga de la plataforma de juego;

- Análisis de la actividad del jugador en partida para detectar si realiza alguna de las actuaciones objeto de control: desbloqueo de objetos indebido, daño excesivo, vista través de paredes, entre otros ejemplos que se expondrán en el apartado 1.4 de funcionamiento;

- Aplicación de sanciones totalmente automatizadas y ajustadas a la gravedad y reiteración en el uso de tratamiento: prohibición de acceso temporal, permanente o pérdida del contenido adquirido, entre otras.; y

- Posibilidad de reclamación por parte del jugador ante las sanciones impuestas. Esta fase la realizaría en exclusiva la propia editora o «*publisher*[12]» del videojuego con la información suministrada por el proveedor del sistema para poder revisar cada caso.

El comentario de los sistemas adicionales referidos en el contexto de grabación de canales de voz y de alternativa de denuncias por el resto de jugadores, como ya se ha indicado en el apartado anterior de contexto, se tratará en apartados separados más adelante. Asimismo, se excluye de análisis los sistemas separados de DMR o gestión de derechos de autor, debido a su componente estricto de control del acceso legítimo desde el punto de vista de propiedad intelectual y su mayor relevancia a efectos de protección de datos.

Se considera de mayor relevancia para el objeto de este estudio centra el análisis en la parte de detección y prevención de los conocidos como «*Hard Cheats*» o trampas en sentido real. Es decir, cualquier dispositivo, hardware o manipulación premeditada del jugador, sea propia o adquirida de un tercero, con el objeto de distorsionar o «*romper*» el equilibrio del juego. En contraposición, estarían los «*soft cheats*» o el uso de fallos, funcionalidades o elementos mal implementados («*glicthes*» o «*bugs*») para obtener

[12] Nombre de la figura en inglés que se usa de manera indistinta para referirse las entidades editoras y a las entidades distribuidoras en videojuegos en España o en cualquier otro país. En alguno supuestos pueden reunir los dos roles, o ser empresas del mismo grupo empresarial, pero lo habitual es que lo desarrollen dos empresas totalmente independientes.

una ventaja[13]. Por este elemento de falta de intencionalidad y de actuación activa, se dejan fuera del objeto de estudio.

Los sistemas antitrampas se aplican en cualquier esfera de juego: consola, móvil u ordenador, pero se considera de mayor relevancia y claridad enfocar el análisis en el entorno de juego en ordenador por la mayor libertad de acceso a los archivos e instalaciones de programas de los que dispone el jugador en este entorno. Asimismo, se considera enfocarlo en el jugado multijugador, al ser la modalidad más jugada y principal sobre la que se enfocan este tipo de sistemas de control.

Intentado obtener la mayor practicidad posible en el análisis que se realizará, el comentario se enfoca en cinco de los grandes sistemas antitrampas de la actualidad. Existe un número mucho mayor de sistemas comercializados a gran escala en la industria, pero se han considerado los siguientes por aplicarse a muchos de los videojuegos de ámbito multijugador más jugados en la actualidad:

- Vanguard, como el sistema propio de Riot Games[14] aplicado en los videojuegos League of Legends o Valorant. Probado sobre el propio juego Valorant;

- VAC, como el sistema propio de Valve/Steam aplicado en los videojuegos Counter Strike Global Offensive, Counter Strike 2 o DOTA 2. Probado sobre el videojuego: Team Fortress 2;

- Easy anti-cheat como uno de los sistemas de tercero más populares, probado sobre el videojuego: Fornite: Battle Royale. Cuyo responsable es Epic Games;

- Ricochet, como uno sistema propio de Activision[15] aplicado a los videojuegos de la Saga Call of Duty. Probado sobre el videojuego: Call of Duty:Warzone; y

- BattlEye, como uno sistema de tercero (*empresa del mismo nombre*) popular que usan multitud de juegos de la editora Ubisoft populares de corte multijugador. Probado sobre el videojuego: Xdefiant, pero cuyo responsable se considerará Ubisoft en este estudio, por ser el titular del videojuego.

Asimismo, se sustituyen las tablas o esquemas por capturas de ejemplos reales de los distintos elementos que se van a exponer. Todo ello con el único objetivo de ilustrar determinados elementos de privacidad comentados, y sin tener en ningún momento intención de que sirva como señalamiento del incumplimiento de ninguna de las entidades titulares.

Para mantener lo máximo posible el enfoque positivo y no de señalamiento, se limitará la referencia concreta en el presente estudio a las entidades citadas en casos muy

[13] En bastante común que, en el lanzamiento de videojuegos de corte multijugador, se implementen mal determinadas características que permiten a los jugadores que las descubran, obtener ventajas o facilidades no deseadas ni previstas. Por ejemplo, que en un nivel bajo exista una misión que dé una experiencia indebida para esa fase del juego. También se considerarían en esta categoría, salvo previsión en los términos y políticas, aquellos jugadores que se aprovechan de cualquier fallo para pasarse el juego de la manera más rápida posible, bajo la práctica denominada «*Speedrun*».

[14] Las entidades referenciadas actuarán como «*responsables del tratamiento*» a efectos del estudio.

[15] La denominación social de la empresa, adquirida recientemente por Microsoft en un proceso complejo de validación de autoridades de competencia por posible obtención de posición de dominio del mercado, es Activision-Blizzard-King. A efectos de simplificación expositiva, se considera referir sólo la 1ª parte de dicha denominación social.

concretos, pero sin perjuicio de la referencia que existiera en toda la documentación de consulta y fuentes utilizadas.

A efectos de simplificar la referencia y aprovechar el hecho de encontrarse asumidas gran parte de las directrices utilizadas[16], se hará referencia exclusiva al Comité Europeo de Protección de Datos («*EDPB», por sus siglas en inglés y denominativo para el presente estudio*) y no al antiguo «*Grupo del Artículo 29*». Asimismo, las referencias concretas a párrafos o páginas de dichos documentos que se citen en notas a pie de página, se realizan sobre las versiones oficiales traducidas al castellano.

En atención a lo dispuesto por la Real Academia de la Lengua Española sobre el calificativo apropiando en castellano, se utilizará durante el mismo el concepto de «*antitrampa*», en lugar del ya referido anglicismo más común en el habla de «*anti-cheat*».

Finalmente, desde un punto de vista terminológico, el concepto «*interesado*» se sustituirá por el de «*jugador*» por ser el concepto más adecuado para referirse al afectado por el tratamiento de sus datos personales en un videojuego.

1.3. Metodología y fuentes utilizadas

Para la consecución del análisis pretendido, el planteamiento de este estudio se basa en los siguientes cuatro puntos:

- Análisis a nivel general de los registros generados durante el juego, mediante la aplicación de programas de monitorización del uso de recursos y actividad en el dispositivo, a fin de poder obtener la mayor certeza posible sobre el acceso a la información que realizarían dichos sistemas antitrampas en el dispositivo del jugador. El detalle de la metodología seguida, programas de medición utilizados y resultados obtenidos, será objeto de análisis en el apartado específico sobre esta cuestión.

- Análisis pormenorizado de las cláusulas informativas, políticas de privacidad, opciones y funcionalidades de privacidad, ejercicio de derechos, así como cualquier otro elemento relacionado al que el autor ha tenido acceso como usuario activo del propio juego, por estar publicado o aportado por el responsable a petición;
- Valoración jurídica de la adecuación de cada uno de esos elementos, en atención al tenor literal de la normativa de protección (*RGPD y LOPDgdd*) y las directrices, informes o guías marcadas por las autoridades a nivel europeo o de otros estados miembros en casos pertinentes; y
- Propuesta de soluciones para aquellos elementos analizados que se considera que no cumplen adecuadamente.

En relación a las fuentes utilizadas para el presente estudio, se referenciarán todos los documentos legales, de autoridades, doctrinales 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 y las capturas citadas en el apartado anterior.

1.4. Funcionamiento de los sistemas antitrampas

A efectos completar el contexto previo de los sistemas antitrampas, se referencia de manera general el funcionamiento de este tipo de sistemas. A efectos generales, existen

[16] Endorsement 1/2018 - GDPR WP29 Documents.

dos grandes familias de sistemas por el lugar en el que realizan el análisis del comportamiento del jugador:

- Del lado del servidor del juego o «*server-side anti-cheat methods*»: un sistema que se centra en detectar cualquier anomalía en el intercambio de información con el servidor del juego que implica la conexión necesaria del dispositivo del jugador para poder acceder; o

- Del lado del cliente de juego o «*side-client anti-cheat methods*»: un tipo de sistema que se centra en el análisis de los archivos del propio dispositivo del jugador en buscar de cualquier anomalía, cambio o programa que se considere una trampa.

Aunque existen ejemplos comercializados de ambos tipos, la gran mayoría responde al segundo enfoque de exigir al jugador un acceso a nivel de administrador de su dispositivo para garantizarse que se analiza cualquier cambio, anomalía o acción que pudiera hacer el jugador. Cuatro de los cinco sistemas analizados, responder a esta tipología, y se conocer de manera general y en la información publicada como «*a nivel de Kernel*» o a «*nivel de anillo cero*».

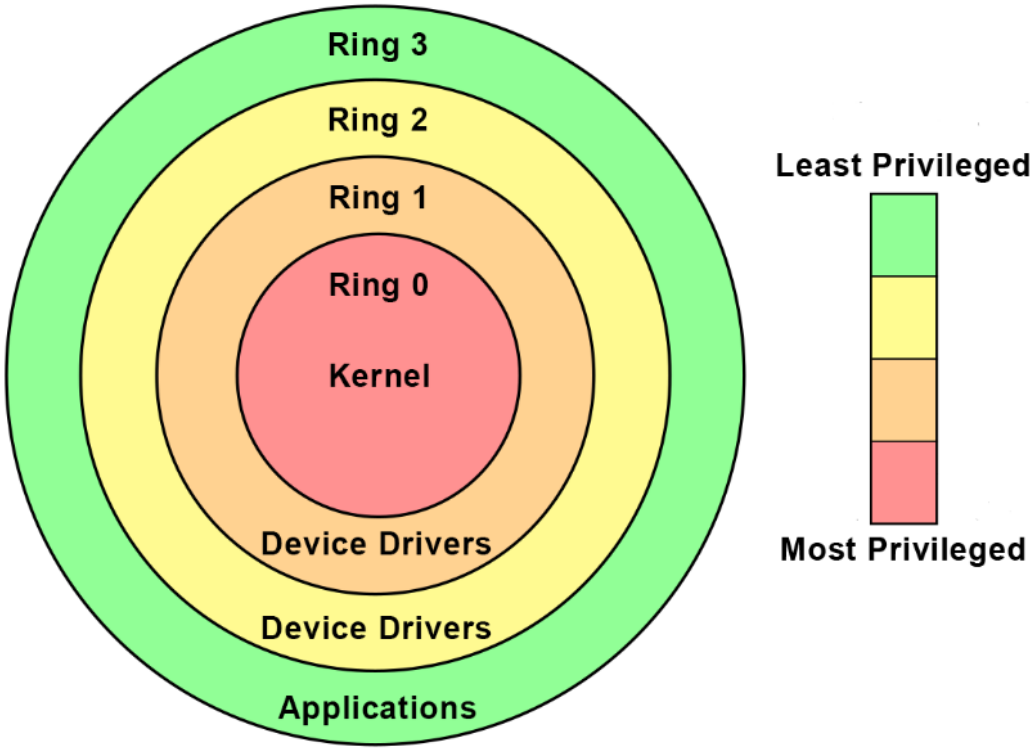


Figura 1. Diagrama de coronas circulares concéntricas que, usualmente, se utiliza para mostrar visualmente los distintos niveles de acceso o privilegios a un dispositivo o sistema. Fuente: «/dev/null: Anti-Cheat Kernel Driver» en el lanzamiento de uno de los sistemas objeto de estudio: Vanguard. Riot Games. 2020.

El uso prioritario de sistemas con este enfoque implica un acceso mucho más intenso a cualquier tipo de información personal y no personal del jugador, impactando de manera clave en su privacidad y protección de datos. Asimismo, el mayor riesgo de seguridad que implica un acceso de nivel máximo de privilegio a un dispositivo, tanto por el acceso indiscriminado, como por la posibilidad de realizar cualquier modificación o alteración sin autorización expresa del verdadero administrador[17].

[17] Este es un elemento que casi todos los sistemas antitrampas reconocen en su información de preguntas frecuentas o comerciales, pero no en la propia información legal puesta a disposición

La mayoría de proveedores de este tipo de sistemas argumentan la necesidad de este tipo de acceso por las siguientes dos razones principales:

- Que un control a nivel de aplicación en modo usuario, por ejemplo, a través de una API o como extensión en un navegador web, sólo permitiría obtener una medición adecuada si el propio jugador comete el error de filtrar información, o se aprovecha una vulnerabilidad del sistema operativo; y

- Que se considera una medida de seguridad adecuada el hecho de que aparezca un aviso de autorización previo al usuario bajo la descripción general tipo de «*¿Desea permitir que esta aplicación realice cambios en su dispositivo?*».

A efectos del funcionamiento propiamente dicho, analizan y escanean el dispositivo y la actuación del jugador a los siguientes efectos:

- El comportamiento del jugador en la partida para poder inferir si está realizado alguna conducta catalogada como una de las funcionalidades que los sistemas de trampas comercializados permitirían hacer al jugador, a fin de imponerle las sanciones previstas por el contrato suscrito con el jugador[18];

  Existe un listado prácticamente inabarcable y en continua actualización, pero a efectos ilustrativos, se pueden destacar los siguientes: apuntado automático o «*aimbot*»; manipulación del disparo para que se haga sin pulsar nada o «*trigger hack*»; ver a través de las paredes o «*wall hacks*»; el retardo artificial para que el servidor no procede el daño del disparo al jugador o «*lag switch*»; alteración de la visión del juego más allá de bajar los parámetros del monitor o «*camera hacks»;* o el acceso a armas sin pasar lo hitos del juego o «*unlocking*»;

- El escaneo de cualquier archivo o modificación que se realice en el dispositivo desde el que el jugador está jugando, a efectos de detectar cualquier cambio, archivo extraño o uso de programas de terceros que pueda afectar de alguna manera; y

- El escaneo de cualquier periférico que se conecte al dispositivo, a fin de poder analizar si se pretende utilizar alguno que pueda alterar el juego o el equilibro en partida de alguna forma[19].

Para poder garantizar el funcionamiento en tiempo real del sistema antitrampas, además del acceso a nivel de administrador o «de kernel» referido, requeriría tres obligaciones adicionales:

- Conexión permanente a internet: es decir, que en todo momento deberá estar autenticado en la plataforma concreta del juego;

---

del usuario: Por ejemplo, Diapositiva 3º del documento «*Q&A about Denuvo Anti-Cheat and Windows Kernel-Mode Drivers* « del conocido denostado por rendimiento y efectividad sistema DENUVO: «*Una vez que el controlador está instalado y en funcionamiento, puede acceder a todos los recursos del sistema sin pedirte permiso a ti, el usuario*.»

[18] El contrato de usuario final o «*EULA*» suele remitir a la existencia del código de conducta y sanciones aplicables, en su caso. Todo ello aceptado por el jugador previamente al juego.

[19] Por ejemplo, mandos de consolas en juego móvil que dan una ventaja en control, o uso de ratón en juegos de ordenador que otorgan la misma ventaja en juegos de disparos o «*shooter*» frente a jugadores de móvil o de consola. Son conocidas las restricciones que el popular juego de disparos del género «*Battle Royale*», PUBG: Battlegrounds, realiza sobre los periféricos laterales de fábrica que incluyen móviles enfocados al público jugador con botones o periféricos adicionales.

- Desactivación o desinstalado de todo programas o elementos que cree conflicto de alguna manera con el sistema antitrampas. Esto implicaría que el jugador tuviera que incorporar excepciones de seguridad en ámbito del cortafuegos, antivirus u optar por desinstalarlo, en casos más excepcionales. Asimismo, en caso de fallo o detección, la denegación del acceso a la propia plataforma de juego, y no sólo al propio juego o modo online; y

- En la mayoría de casos, el establecimiento por defecto del sistema como una aplicación de arranque del dispositivo[20].

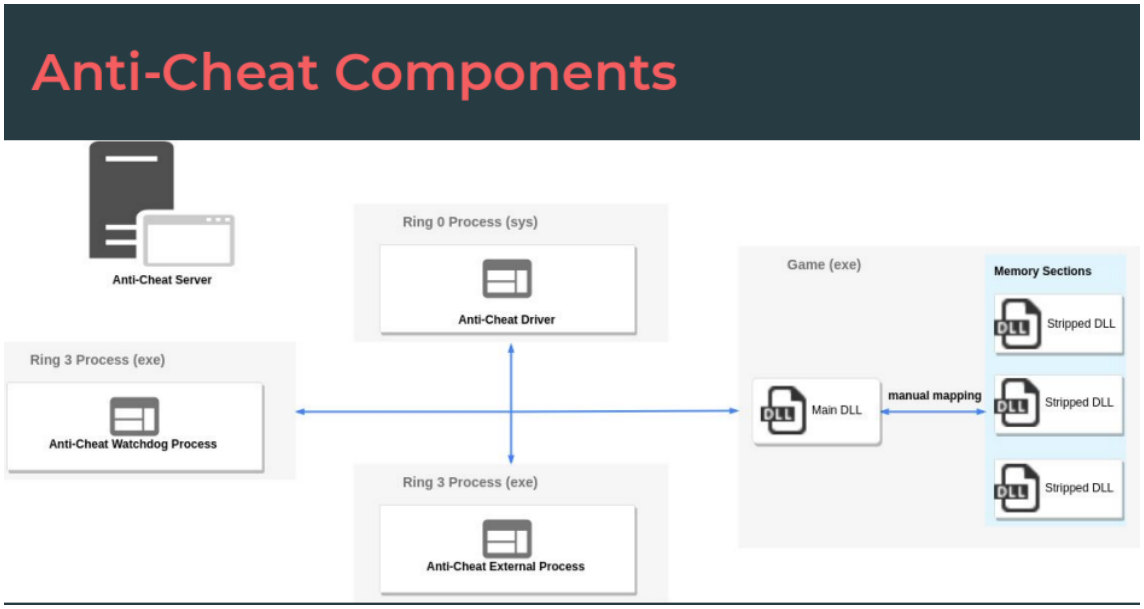


Figura 2. Gráfico general que muestra la imagen tipo del funcionamiento de este tipo de sistema a nivel de kernel: instalación a nivel 0 o de administrador para garantizar el acceso total y medición a otros niveles de privilegios de las aplicaciones y archivos del dispositivo, a nivel del propio juego en el sistema y con el envío de información al servidor del mismo. Autor: Joel Noguera, Security Consultant at Immunity Inc. Fuente: Unveiling the underground world of ANTI-CHEATS. REcon MONTREAL 2019, Diapositiva nº 13.

2. Estudio

2.1. Análisis de los registros generados

Con el objetivo de intentar obtener información actualizada, lo más exacta posible y específica de cada caso, se ha procedido a realizar una sesión de juego por cada título. En cada una de dichas sesiones, se han activado dos sistemas paralelos de medición en tiempo real de los eventos que provocan en el dispositivo cada sistema antitrampas y cada plataforma de juego sobre la que se configura. Dichos sistemas de medición utilizados, son las dos herramientas propiedad de Windows Sysinternals siguientes:

- **Process Monitor (*conocido comúnmente como «Procmon»*):** herramienta que permite monitorizar en tiempo real los registros, sistemas de archivos y actividad de los procesos o subprocesos de Windows, durante el tiempo que se decida activar; y

[20] En 2020, provocado por el lanzamiento de la primera versión del sistema antitrampas «*Vanguard*» para el juego «*League of Legends*», se produjo un fuerte rechazo por parte de los jugadores a la obligación de que el sistema fuera una aplicación de arranque. Ante esto, se estableció la posibilidad de desactivación como de arranque, que se ha quedado como medida para el resto de sistemas a futuro.

- **System Monitor (*conocido comúnmente como «Sysmon»*)***:* herramienta que permite registrar información sobre la creación de procesos o las conexiones de red en tiempo real, al ser un sistema que se configura como una aplicación de arranque del dispositivo, es decir, que siempre está activo.

El uso de estos sistemas no podría considerarse como un análisis forense[21] que permitiera, idealmente, extraer el conjunto de datos personales o información concreta accedida, a fin de cotejarlo en relación directa con el conjunto de datos personales que cada sistema reconoce tratar en la información al jugador. A pesar de esta limitación de base, se ha considerado el uso de estos sistemas limitados por las dos siguientes razones:

- Al ser suministrados por Microsoft para el entorno específico de Windows sobre el que se realiza la medición, existe menos probabilidad de causar algún problema, conflicto o funcionamiento inadecuado que otros sistemas o herramientas de terceros; y que

- Los sistemas antitrampas, además de su actividad principal de detección de trampas, incluyen detección de sistemas de análisis profundo o similares que pudieran de alguna manera extraer información o inferencias del funcionamiento o código fuente. Todo ello se realizaría en el marco de una medida de protección tecnológica para evitar que sea posible vulnerarlo o copiarlo, pero provocando los dos siguientes efectos: el mal funcionamiento del juego, o su imposibilidad de carga completa[22]; y la consideración como una trampa, con la subsiguiente restricción o sanción por incumplimiento contractual.

Por todo lo dicho, se indican los siguientes resultados principales de los registros o «logs» generados que confirman el acceso completo al dispositivo[23]:

- Se constata la existencia del acceso a nivel de administrador al dispositivo y al núcleo, por las siguientes rutas identificadas:

- «*NT AUTHORITY\SYSTEM*»: acceso completo al sistema a nivel de los servicios del propio sistema operativo y controladores;

- «*HKLM (HKEY_LOCAL_MACHINE)*»[24]: acceso a la raíz del registro de Windows que contienen la configuración y la información específica del usuario que sólo se puede acceder con autorización específica a nivel de administrador. En específico, lo siguiente:

    - Datos de inicio de sesión en aplicaciones;
    - Historial de navegación y preferencias;

[21] Herramientas o programas como los conocidos «Wireshark» para el análisis de protocolos y redes de comunicación, o «Volatility» como herramienta más enfocada en el análisis de la memoria RAM.

[22] No existe una estandarización a nivel de la industria sobre los tipos de mensajes de error que le aparece al jugador, ni que se especifique en todos los casos que es un fallo provocado por un programa concreto. Como ejemplos más usuales, se pueden destacar los siguientes: error sin aviso de ningún tipo, mensaje de error genérico, mensaje de error concreto referido al sistema antitrampas sin más explicación, o un mensaje codificado que obliga al jugador a acudir a la web oficial para consulta la tabla de correlación correspondiente.

[23] Accesibles para su consulta en formato CSV, a través del enlace materiales del apartado de contexto, o del enlace dispuesto a tal efecto en el apartado de bibliografía y materiales.

[24] Acceso concreto a las siguientes rutas: HKLM\System\CurrentControlSet\Control\Session Manager, HKLM\System\CurrentControlSet\Control\Nls\SortOrder o HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion.

- Configuraciones personalizadas que pueden incluir información de identificación personal;
- Configuraciones de software instalados;
- Preferencias de usuario;
- Configuraciones de escritorio;
- Configuraciones de red; o
- Información de inicio de sesión.

- Que existe extracción de información fuera del dispositivo, a pesar de que alguno de los sistemas analizados en su información declara que no sale de información del dispositivo, mediante la existencia de las operaciones «*TCP Send*» o «*TCP Receive*» con conexión a direcciones externas.

- Que el hecho de tener acceso a nivel de administrador permitiría realizar operaciones en consonancia con el nivel de acceso máximo. En el apartado relativo al interés legítimo se valorará si la legítima expectativa del jugador llegaría a un acceso a este nivel con potencia de control total, pero con dicho nivel de privilegio se constata que podrían realizar operaciones como las siguientes:

  - Modificar o eliminar archivos del sistema;
  - Instalar o desinstalar software;
  - Cambiar configuraciones del sistema; o
  - Crear, modificar o eliminar cuentas de usuario.

A esta limitación de medios de análisis técnico no bloqueables para extraer la información personal concreta tratada, se suma el elemento de que no ha sido posible, como se indicará en el apartado 2.2.6 sobre derecho de acceso, obtener copia de los datos personales objeto de tratamiento concreto.

Finalmente, el único elemento de detalle sobre los datos personales tratados es el indicado en la información puesta a disposición del jugador. Se declara un nivel de acceso completo en el sentido comentado, pero de manera que un usuario sin conocidos técnicos o de protección de datos pueda hacerse a la idea de un acceso completo al dispositivo[25]:

- *Sitios web visitados antes y después de utilizar una Propiedad;*
- *Tipo de navegador e idioma;*
- *Dirección IP;*
- *Información del hardware y software (por ejemplo, números de serie);*
- *Datos de juego (por ejemplo, nombre en el juego, ID de cuenta, etc.);*
- *Comunicaciones (incluidas, de manera no exhaustiva, las comunicaciones de chat, texto o voz);*
- *Información sobre el sistema operativo en ejecución;*
- *Información sobre procesos en ejecución, controladores y otros códigos ejecutables;*
- *ID de publicidad móvil, identificadores no personales y otra información de su dispositivo móvil;*
- *Información sobre archivos y memoria relacionados con el juego y con el sistema operativo; y*
- *Nombres de archivos incluidos en otra información, que también pueden contener el nombre de usuario de su sistema operativo*

[25] Combinación de la información más concreta facilitada por los sistemas de BattlEye y Ricochet, sobre la tipología de información objeto de tratamiento.

2.2. Análisis desde el RGPD

Con el objetivo de mantener la claridad explicativa y practicidad pretendida, el análisis desde el punto de vista de protección de datos, se realizará sobre la base de las siguiente dos pautas expositivas:

- Cada apartado se corresponderá con cada elemento de información que los artículos 13 y 14 del RGPD determinan para que el interesado sea claramente informado. Asimismo, en cada uno de ellos se comentará la información de las políticas que correspondiera por cada elemento. Es decir, la ordenación que se considera más habitual y estandarizada a nivel de información y políticas de privacidad; y

- En cada uno de estos apartados, se analizará desde esa perspectiva el cumplimiento de los cinco sistemas antitrampas en conjunto, a fin de evitar de una reiteración del mismo comentario con ligeros cambios por el contexto de cada sistema.

2.2.1. Responsabilidad, corresponsabilidad y de encargo del tratamiento

Teniendo en cuenta el esquema de sociedades cruzadas entre el titular del juego y el proveedor del sistema, de lo dispuesto en el RGPD, de las resoluciones del Tribunal de Justicia de Unión Europea (TJUE) relevantes (*Wirtschaftsakademie, Jehovan Todistajat y Fashion ID*)[26], de las Directrices 1725/2018 sobre los conceptos de responsable, encargado y corresponsable del EDPS y las Directrices 07/2020 sobre responsables y encargado del EDPB; cabría empezar el análisis de protección de datos por determinar si se tratarían de responsables, corresponsables o encargados sobre dicho tratamiento.

En el presente tratamiento, existirían tres actores principales:

- **Editora del videojuego o «Publisher»**: entidad titular de los derechos de explotación del título, así como de la plataforma digital en la que el jugador se autentica y procede a jugar al título que considere en cada momento. Lo habitual, es la existencia de una plataforma por cada biblioteca de juegos titularidad de cada editora;

- **Proveedor del sistema antitrampas**: la entidad propietaria y comercializadora del sistema de prevención que pone a disposición de la editora por el acuerdo alcanzado al respecto; y

- **Estudio**: entidad que desarrolla el videojuego y lo gestiona en postlanzamiento, especialmente, en aquellos casos en los que existe un fuerte componente de juego online competitivo o cooperativo.

La figura del estudio, en el marco de este ámbito, siempre va a ser de un mero encargado del tratamiento por cuenta de la editora para implementar el sistema dentro del juego que ha desarrollado y del que realiza el mantenimiento y gestión[27]. Asimismo, el supuesto de los sistemas antitrampas analizados de Riot Vanguard, Easy anti-cheat, VAC y Ricochet, son un claro ejemplo de tratamiento realizado a nivel de responsable en interno de Riot Games, Epic Games, Valve y Activision-Blizzard-King,

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

[27] Puede que, en algunos casos, el estudio sólo desarrolle el juego y no se encargue de ninguna otra labor, o que el estudio y la editora pudieran ser el mismo; pero se considera de esta manera para facilitar la exposición.

respectivamente, o en su caso, de encargado del tratamiento por ser un filial dentro del mismo grupo empresarial.

En el supuesto restante de BattlEye como servicio de tercero prestado a la editora Ubisoft[28], podrían existir dudas legales sobre la relación entre las partes. En la información suministrada al jugador en las políticas de privacidad de ambos, se declara que cada entidad es responsable independiente:

- En el caso de la política de Ubisoft se declara la relación típica de responsabilidad en el tratamiento con proveedor designado como encargado; pero

- En la política de privacidad del proveedor BattlEye, se estipula la declaración de responsabilidad y una comunicación de los datos personales e información no personal a la cliente editora contratante.

Al jugador se le muestra, al inicio y en la instalación del sistema, un cuadro informativo sobre la recopilación de determinados tipos de datos personales[29], así como la indicación a ambas entidades y el enlace a ambas políticas de privacidad. Aunque sin declarar en ningún momento si ambas son responsables independientes, corresponsables o existe alguna relación de encargo de tratamiento.

En aplicación del análisis fáctico que recomienda el EDPB a la hora de poder delimitar qué figura corresponde a cada tratamiento concreto[30], cabe determinar que no sería una relación de encargado de tratamiento como indica Ubisoft. No lo sería porque el proveedor BattlEye no se limita a un tratamiento de los datos personales bajo instrucciones de Ubisoft para ello, sino que se realizará finalidades propias sobre los mismos datos personales. Por ejemplo, utilizarlos con fines de mejorar del sistema que ya haría que excediera la propia figura[31].

Tampoco podría determinarse, con la información existente accesible, que pudiera considerarse una relación de corresponsabilidad. Al menos en las fases de análisis del dispositivo y de la partida del jugador, conclusión y comunicación de la información a Ubisoft para su posible sanción. No se podría justificar que ambas entidades son las que determinen los fines del tratamiento (*el análisis de las acciones y dispositivo del jugador para detectar, analizar y aplicar sanciones por el uso de trampas*) y los medios a aplicar (*el propio sistema antitrampas de tercero con figurado sobre el sistema del editor);* por cuanto *es Ubisoft la que decide establecerlo, y BattlEye proveer un sistema adaptada a la necesidad[32]; y*

Lo ya comentado de que se excedería de la figura del encargado de tratamiento limitada a las instrucciones de responsable con fin propio, pero sin que puede indicar más que

[28] Aplicable a cualquier sistema antitrampas de tercero, que, por motivo de concreción y selección de los juegos más populares de ámbito multijugador, se han dejado fuera del estudio. A efectos ejemplificativos y por popularidad: Denuvo, MHYPROT, Game Protect Game Guard, Punkbuster o Faceit.

[29] Captura denominada «*BattlEye al iniciar 1*» en la carpeta en nube de materiales.

[30] Punto 52, pág. 21, de las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD. Versión 2.0. Adoptada el 7 de julio de 2021.

[31] Artículo 28.10 del RGPD y punto 81, pág. 29 de las referidas directrices sobre responsables y encargados referidos: *«Actuar «por cuenta de» alguien también significa que el encargado no puede llevar a cabo el tratamiento para sus propios fines».*

[32] Este hecho no se desvirtuaría por el supuesto en que Battleye tome decisiones sobre «*medios no esenciales*» del tratamiento para ajustarlo en base al conocimiento del servicio que presta, de conformidad a lo dispuesto por el EDPB en las referidas directrices, puntos 39 a 41, págs. 16 a 18.

ese punto de no responder a sometimiento limitado a contrato de encargado de tratamiento.

2.2.2. Finalidades y bases de legitimación

El tratamiento realizado por los sistemas antitrampas tiene la finalidad de prevención, detección y sanción del uso de cualquier trampa realizado por un jugador. A efectos aclaratorios, ya se han indicado las cuatro fases u operaciones en las que podría secuenciarse para dicho fin.

De conformidad a lo establecido en el artículo 5.1. b del RGPD, en la Opinión 2/2013 sobre limitación de la finalidad[33] y las Directrices 4/2019 de privacidad por diseño y por defecto[34] del EDPB; la finalidad sólo sería legal si cumple tres requisitos principales: estar determinada, ser explícita y ser legítima.

Confrontando dichos requisitos con lo informado en las políticas de privacidad de los sistemas antitrampas analizados, cabría determinar lo siguiente:

- Se concreta en todos los casos el fin perseguido de manera suficientemente específica, determinando en todos los casos que no sólo es una finalidad general de prevención de fraude o vulneración de derechos de propiedad intelectual o de seguridad informática[35], sino aclarando la existencia de sistemas antitrampas para dicha finalidad más concreta: «*prevención y detección del uso de software de trampas con el objetivo de garantizar un entorno de juego justo, tal y como pretende el editor del juego*.»;

- Es un elemento conocido por el grueso de los jugadores, pero sólo en la mitad de las políticas se es explícito en la descripción de cómo se va a proceder a realizar esta finalidad: «*Estos servicios pueden recopilar y analizar datos sobre su ordenador y el software que este tiene para detectar trampas*». Sólo en el caso específico de Riot se establece una descripción más precisa: *«(como software antitrampas que se ejecuta en segundo plano en los dispositivos), que pueden tomar decisiones de manera automática (como suspensiones de cuenta temporales o permanentes, restricciones de la comunicación, eliminación de contenido o acceso limitado al contenido de los juegos)».*

  En el resto de casos, se reconduce a información concreta en documentos separados y no mostrados al jugador en el momento de instalación y 1º inicio, denominados preguntas frecuentes *(«FAQS», por sus siglas en inglés), o información de soporte[36];*

[33] No es de los directrices asumidas del Grupo del Artículo 29 («*Endorsement 1/2018*»), pero se considera su referencia por contener elementos fácticos que son de aplicación efectiva para el supuesto tratado.

[34] «*Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto Versión 2.0 Adoptadas el 20 de octubre de 2020*».

[35] Uno de los ejemplos que el Grupo del Artículo 29 da en dicha opinión de finalidades generales y «*vagas*» que no cumplirían con el criterio de especificidad. Junto con otros ejemplos de fines típicos que prácticamente todas las autoridades de protección de datos nacionales, en base a guías, publicaciones o resoluciones, también consideran improcedentes y contrarias al principio de transparencia y de limitación de la finalidad: «*mejorar la experiencia de los usuarios*», «*fines de marketing*», «*fines de seguridad informática» o «investigación futura*».

[36] El punto más habitual es que la información más concreta se encuentre de manera externa al juego, es decir, que obligue al jugador a realizar una búsqueda en la web oficial de la editora, o en la propio web o información publicada en internet del propio proveedor del sistema antitrampas.

- En todos los casos, se considera que dicha finalidad persigue el cumplimiento de objetivos que se consideran como «*aceptables en virtud de la ley*». A continuación, en la valoración de las bases de legitimación, se ahondará más en este punto intrínsecamente relacionado por el interés legítimo que se alega para ello, aun cuando la finalidad y el interés legítimo son dimensiones distintas[37]:

En cuanto a las bases de legitimación que habilitarían a llevar a cabo este tratamiento de prevención de trampas, de conformidad al artículo 6 del RGPD, se podría considerar, las siguientes tres: consentimiento, ejecución del contrato e interés legítimo. En todos los casos, a excepción de Riot que aporta una triple base de legitimación[38] (*contrato por control del cumplimiento de los términos suscrito con por el jugador, obligación legal para mantener la seguridad e interés legítimo para «comprender cómo se utilizan los Servicios de Riot, garantizar su seguridad y mejorarlos»)*, se opta por el interés legítimo.

Consentimiento

El tratamiento antitrampas, como ya se ha indicado en el apartado 1.4, se configura de manera que se pide una autorización genérica y obligatoria para que el jugador administrador del dispositivo valide que el sistema obtenga un nivel de acceso de administrador para instalarlo y proceder al escaneo. Esta autorización no responde en modo alguno a un consentimiento en materia de protección de datos, pero es un indicativo de que basar el propio tratamiento en esta base de legitimación, implicaría cierta problemática real.

De conformidad a 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[39], el consentimiento en este tratamiento específico podría resultar inadecuado por las siguientes razones:

- **Libertad:** se configuraría como una exigencia ineludible y sujeta a los términos del contrato[40], distorsionando la capacidad de elección que el jugador necesitaría tener para que fuera una base legal. Asimismo, no se establece en ningún caso, sea de los analizados o cualquier otro, un sistema alternativo de control de trampas que permitiera que el jugador eligiera de manera real. Tampoco a nivel de intensidad del control ejercido; y

- **Revocabilidad:** no existiría una verdadera retirada del consentimiento sin los efectos negativos o perjuicios para el jugador ya comentados anteriormente: la imposibilidad, no sólo de acceder a partida con otros jugadores, sino también a no poder abrir correctamente el propio juego[41]. Este perjuicio no sólo se daría en el caso de que se decidiera no instalar o configurar correctamente el sistema, sino que alcanzaría a que el jugador tuviera que desactivar o desinstalar todos

[37] Tal y como recuerda el EDPB, en su «*Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*», 1º párrafo, pág. 29.

[38] Elemento que contraviene el RGPD al no declarar de manera exacta qué base de legitimación aplica al tratamiento concreto. Unido al elemento de confusión que implicaría que se declare que la seguridad se hace en base a una obligación legal no declarada en norma con rango de ley pertinente, así como un interés legítimo que también hace referencia a la misma finalidad de seguridad.

[39] «*Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 versión 1.1 adoptadas el 4 de mayo de 2020*»,

[40] Una de las advertencias que el EDPB da en sus directrices citadas 05/2020 como un elemento que denota que no existiría una libertad real de consentimiento. Punto 13, pág. 7.

[41] Justo el punto concreto que el EDPB en dichas directrices de consentimiento estipula como ejemplo de no existencia de consentimiento: «*por ejemplo, sin que disminuya el nivel en la prestación del servicio en detrimento del usuario*». Punto 48, pág. 12.

los restantes programas o funcionalidades que causarán algún tipo de conflicto o error.

En algunos casos se argumenta que sí se otorga un control al jugador por poner a su disposición un botón o aplicación especifica en segundo plano consultable y desinstalable (*por ejemplo, el que otorga Riot*[42]), pero se considera que sería una medida de carácter formal cuya desactivación o desinstalación activaría los efectos negativos o perjuicios indicados.

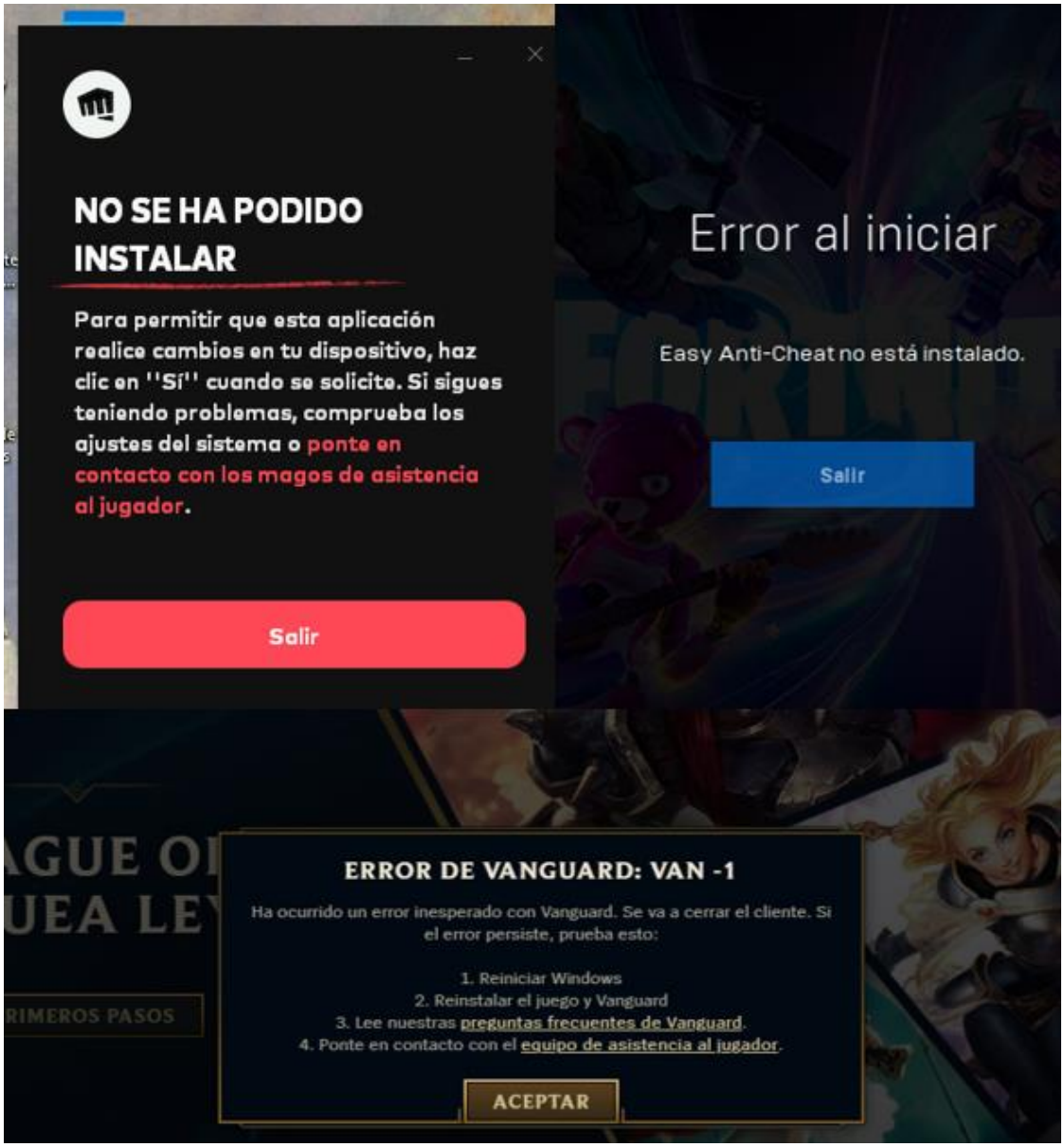


Figura 3. Combinación de tres capturas de mensajes que los sistemas antitrampas, Vanguard (arriba-izquierda y abajo) e Easy Anti-cheat (arriba-derecha), muestran al jugador en caso de error o no autorización del sistema. En el primero de los casos, incitando al usuario a consentirlo de manera directa.

Desde el punto de vista del responsable, tampoco se considera una base adecuada que permitiera realizar una finalidad que se considera legítima, siempre y cuando se configure y limite adecuadamente. El otorgar al jugador la capacidad real de decidir si consiente o no un tratamiento que implica un control y sanción, supondría un fuerte

[42] Dicho botón se implementa como una aplicación separada y en 2º plano que permite esta desinstalación formal y descargar los logs cifrados para remitir a soporte ante problema técnico.

rechazo y la imposibilidad de real de llevarlo a cabo. Asimismo, el darle una suerte de impunidad (*o de amenaza de acudir a las autoridades de protección de datos*) a los posibles jugadores tramposos para nunca ser sancionados antes conductas lesivas para terceros y contrarias a los términos del servicio.

Ejecución de un contrato

Una de las bases más utilizadas para intentar legitimar todo tipo de tratamientos que devengan de un servicio o de la relación contractual con el jugador. En el presente caso, como ya se ha indicado, en uno de los supuestos se basa el tratamiento antitrampas en la vigilancia del cumplimiento del contrato suscrito.

De conformidad a lo dispuesto al Considerando 44, el artículo 6.1.b del RGPD, y las Directrices 2/2019 del EDPB sobre esta base de legitimación[43], se considera que el elemento nuclear de necesidad de esta base no podría justificarse en este caso concreto por lo siguiente.

- **Necesidad**: el presente tratamiento, aun cuando se intente justificar por la necesidad de seguridad en sentido amplio, no respondería al elemento de ser completamente imprescindible u «*objetivamente necesario*» para prestar el servicio que el jugador contrata. Por ejemplo, se consideraría entendible esta necesidad en el tratamiento de datos personales y no personales para el emparejamiento de jugadores en partida, en base a ofrecer funcionalidades de juego online o multijugador[44];

- **Insuficiencia como cláusula en el contrato:** la pauta, recordada por el EDPB, de que la interpretación de dicha necesidad tiene que ser estricta y no comprende situaciones en la que se imponga de manera unilateral por el responsable en el acuerdo suscrito[45]; y la

- **Inaplicación de la petición precontractual**: el jugador no solicita en ningún momento la aplicación de medidas previas tendentes a asegurar que se lleve a cabo este tratamiento como parte del servicio contratado, ni podría justificarse que fuera una actuación adecuada imprescindible para poder llevarlo a cabo en un futuro. La petición del jugador podría ser que se lleven a cabo las medidas necesarias para asegurar que su juego se realice en condiciones adecuadas, pero no alcanzaría a este nivel que implicaría el tratamiento de datos de terceros jugadores para lograrlo[46].

[43] «*Directrices 2/2019 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. Versión 2.0 8 de octubre de 2019*». En el «*2º informe relativo a la aplicación del RGPD*» de la Comisión Europea, de 25 de julio de 2024, se reconoce la necesidad de directrices adicionales sobre dicha base de legitimación, así como en materia de anonimización y seudonomización, o sobre investigación científica. Último párrafo, pág. 7.

[44] Este concepto comprendería cualquier configuración de juego en línea: contra otros jugadores o por equipos o en modo cooperativo contra enemigos virtuales generados por el propio juego (*conocidos habitualmente como «jugar contra la inteligencia artificial o IA*»).

[45] Punto 28, pág. 10 de las referidas directrices 2/2019.

[46] El EDPB recuerda en el punto 46, pág. 14 de las mencionadas directrices 2/2019, el hecho de que podría justificarse en esta base si el interesado lo solicita y es algo conectado, aun cuando no fuera estrictamente necesario para llevarlo a cabo.

Interés legítimo

Entrando en la valoración jurídica de la base principal alegada por los sistemas analizados, de conformidad al artículo 6.1.f, el Considerando 47 del RGPD y las Directrices 06/2014 de esta base de legitimación[47], se puede plantear lo siguiente.

No se ha tenido acceso a la copia de la evaluación de interés legítimo que se debería haber realizado en cada caso objeto de estudio, pero con la información puesta a disposición y el funcionamiento del sistema sobre el jugador, se considera que se tienen suficientes elementos para realizar una valoración adecuada:

- **Legitimidad del interés pretendido:** en un primer vistazo de la información puesta a disposición en la política de privacidad, podría entenderse que el objeto de «*mantener el juego libre de usos indebidos malintencionados, abusos o trampas*» fuera un interés apremiante y beneficioso para la sociedad (*la parte de ciudadanos que juegan habitualmente),* pero, a efectos, sería un interés más enfocado en el ámbito económico/empresarial del propio responsable para mantener un entorno de juego atractivo para que sus clientes sigan entrando al mismo, así como limitar los posibles efectos legales por reclamaciones a nivel de consumidores;

  Sí se consideraría un interés legítimo objetivo de base, de conformidad a responder claramente a uno de los supuestos especificado en este sentido por el EDPB en las citadas directrices del interés legítimo: «*la prevención del fraude, el uso indebido de servicios o el blanqueo de dinero*». La información puesta a disposición del jugador, va en esta misma línea de destacar la prevención de fraude, junto con la delimitación de aplicarse al ámbito de la partida y del dispositivo del jugador.

  Asimismo, respondería a los elementos necesarios de ser lícito (*no estar prohibido por la normativa y tener el elemento de relación evidente con las medidas de protección tecnológica de propiedad intelectual*), estar articulado con claridad suficiente (*en la mayoría de los supuestos analizados sin ser el mismo contenido de la finalidad a la que se refiere*) y represente un interés real y actual (*una necesidad real de la industria y que puede implicar perjuicio para el responsable*).

- **Legítimas expectativas:** teniendo en cuenta que las legítimas expectativas han de poder deducirse por sí mismas sin necesidad de aclaración o matización[48], podría argumentarse que es un tratamiento conocido y esperado por cualquier jugador habitual de videojuegos, a nivel de que en el tiempo de partida se le monitorizará para sancionarle por trampas.

  El punto de problemática es que los jugadores no tienen información suficiente para conocer en detalle esa 1º fase de escaneo en tiempo real de su dispositivo previo a la partida y a la apertura del propio juego, más allá del mensaje genérico de autorización de acceso a nivel de administrador si decirlo ya referenciado, o la indicación en las pantallas de instalación y 1º acceso de la existencia del sistema concreto aplicado. Para poder conocer el alcance real del mismo, el jugador necesitará consultar la información de preguntas frecuentes o detallada en página separada que no se muestra en el acceso habitual del mismo;

- **Necesidad**: partiendo de que el concepto de necesidad aplicado al interés legítimo no debe interpretarse como un sinónimo de «i*ndispensable*», ni tiene la flexibilidad

[47] Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE. Adoptado el 9 de abril de 2014.
[48] Elemento recordado por la AEPD en su resolución sancionadora del BBVA (*PS/00070/2019*). Párrafo 3º, página 104.

de conceptos como «*admisible*», «*útil*» o «d*eseable*»[49]; cabría plantearse si superaría el juicio de ponderación en este punto, al concurrir varios hechos:

- **Existencia de alternativas menos invasivas** para lograr la pretendida finalidad de prevención de trampas, así como el perjuicio al jugador por antivirus, programas legítimos o cortafuegos de los que se exige su desinstalación o desactivación. En este punto en particular, podrían considerarse tres elementos concretos:

  - La existencia de la 2ª operación o fase de tratamiento de monitorización en partida para detectar las actuaciones ejemplificadas en el apartado 1.4 (*apuntado automático, inclusión de lag, o visión a través de paredes, entre otras)*, que, llevada a cabo de manera autónoma, cumpliría la misma finalidad pretendida. En la línea del argumento expuesto de interés más económico/empresarial sobre la legitimación, esta 1ª fase de escaneo preventivo serías las susceptible por de interpretarse como no tan ponderada y más sujeta al interés del responsable de dotarse de un escenario de gestión preventiva indiscriminado que permita detectarlo antes de la comisión de cualquier infracción.

  - En el apartado de contexto se ha expuesto la alternativa de sistemas que miden la interconexión entre el jugador y el servidor en el que se ejecuta el juego, pero sin acceso más allá de eso. Por ejemplo, el sistema VAC de Valve, dentro de los cinco analizados en el presente estudio; o

  - La propia posibilidad de denuncia y revisión que se da a otros jugadores, pero con la particularidad añadida de que fuera con supervisión humana en la propia fase de denuncia y sanción, y no sólo en la de posible reclamación por el infractor sancionado. Se comentará con más detalle en el apartado 2.4 relativo a dicha especialidad de denuncias de otros jugadores.

- **La efectividad real de este tipo de sistemas** podría no considerarse suficiente para poder justificar un nivel de acceso tal al dispositivo de todos los jugadores, con independencia de si en algún momento hubieran vulnerado los términos y condiciones en este sentido. De manera pública y general, los medios se hacen eco con cada nuevo videojuego de gran presupuesto del tiempo de días, semanas o meses que se tardan en superar los sistemas antitrampas implantados en los mismos[50].

  Asimismo, la faceta relacionada del fallo del sistema que asigne sanciones indebidas a jugadores que no hayan realizado trampa alguna, y que obligue a iniciar un proceso de reclamación con el perjuicio no procedente ya aplicado. Por ejemplo, al asumir que una mala conexión continua en partida o partidas se debe no a ese hecho, sino a un intento de manipular al servidor para que no procese en tiempo real el daño recibido por el jugador.

  Sin olvidar el elemento adicional de que multitud de usuarios en redes sociales muestran sistemas de trampas totalmente analógicos y efectivos que serían

[49] Interpretación dada del concepto por el Tribunal Europeo de Derechos Humanos (TEDH) en su apartado 97 de su Sentencia de 25/03/198, y recordado por la AEPD en su PS/00070/2019, 4º párrafo, pág 125.

[50] A tal punto, que entidades como la titular del sistema Vanguard, Riot, otorgan recompensa a aquellos especialistas que consigan vulnerar su sistema. Todo ello en el marco de los conocidos «*bug bounty*» o búsqueda de problemas de seguridad que son práctica habitual en múltupleas empresas de tecnología y ámbito digital.

indetectables para cualquier de sistema antitrampas actual. Por ejemplo, el añadido de determinados objetos o lupas de aumento en algún soporte externos que amplía el punto de mira, pintado externo de la pantalla para aumentar la retícula del arma, o manipulación de los parámetros de iluminación, contraste o adición de elementos visuales que permita el monitor o pantalla desde la que se juegue[51].

- **Los riesgos de seguridad inherentes al acceso a nivel de administrador**: el enfoque pretendido, especialmente en los casos en los que sea una aplicación de arranque, o en los que el jugador haya guardado la sesión para que tras el encendido se active el cliente de juego, pueda servir como pasarela para cualquier ataque informático. Cualquier ataque exitoso en los sistemas del editor o del titular del juego, daría acceso automático al dispositivo y archivos del jugador sin restricciones y de manera imperceptible para el mismo;

- **Proporcionalidad:** del otro elemento principal del juicio de ponderación que obliga a analizar el impacto en los derechos y libertades del interesado, a fin de establecer garantías y límites concretos para minimizar su daño y seguir permitiendo realizar el tratamiento, se considera si también lo superaría por darse los siguientes elementos:

    - La aplicación del principio de minimización[52] al presente tratamiento que alcanza a una observación del dispositivo en tiempo real a máximo nivel de acceso: información sobre el sistema operativo en ejecución, archivos y memoria relacionados con el juego y con el sistema operativo, procesos en ejecución, uso de recursos y memoria del dispositivo o estado de actualización del mismo[53]. Sólo en el caso de BattlEye se concreta en la información de su política de privacidad y de la información usuario en el momento de la instalación, que sólo se almacenara la información en caso de que se detecte un positivo por trampa;

    - El hecho de que el escaneo del dispositivo no se limite a los estrictos archivos y carpeta del propio juego, estableciendo sólo en los casos analizados de BattlEye y de Ricochet que el sistema estará activo durante el tiempo de juego. En el caso de Vanguard, ya se ha comentado que es una aplicación de arranque del dispositivo que siempre está activa sin posibilidad de modificación del parámetro sin efectos invalidantes de juego.

      Sí se considera una medida adecuada de proporcionalidad concreta, que, en el caso concreto de Ricochet no se imponga una penalización adicional al infractor más allá del bloqueo; sino que se equilibre por la vía de dar al resto de jugadores en partida beneficios que anulen la ventaja injustificada detectada: ocultación de los jugadores legales frente a los jugadores tramposos, desactivación de armas

[51] Se llama la atención de que este último sistema, por hacerse en un elemento de hardware del dispositivo, podría ser un elemento detectable y analizable en posibles cambios por el sistema antitrampa.

[52] Con posible incidencia en los principios de principios de Integridad, confidencialidad, y limitación del plazo de conservación por el riesgo inherente en la recopilación de grandes cantidades de información del dispositivo en tiempo real.

[53] La entidad Riot, en documentación de carácter más técnico, indica el hecho de que el sistema Vanguard puede interpretar la no actualización del sistema operativo (*o un sistema antiguo*), como un dispositivo proclive a ser un entorno de instalación de trampas al que bloquear el acceso al juego. «*Si encontramos PCs demasiado aptos para hacer trampas (por ejemplo, debido a un Windows obsoleto o a configuraciones específicas que favorecen la posibilidad de hacer trampas), Vanguard restringirá el acceso de ese PC a VALORANT y mostrará un mensaje de error. El mensaje de error VAN: RESTRICCIÓN le indica qué ajustes son necesarios para eliminar la restricción*.»

y el equipamiento en partida u otorgamiento de un escudo de protección a los jugadores legales[54].

A efectos de mera referencia, se menciona el elemento de la selección de partidas entre jugadores de un nivel similar («*matchmaking*»), como filtro para clasificar en función de su «*comportamiento*» y concentrar a todos aquellos considerados tóxicos por su historial de sanciones, denuncias o reclamaciones, en una misma partida separada del resto. Un elemento que, a diferencia del anteriormente mencionada de proteger con ventajas a los jugados legítimo, podría ser un posible elemento de discriminación a ponderar para los infractores; y

- El elemento problemático de valoración que supone que gran parte del tratamiento se deba realizar por medidos totalmente automatizados que impongan, sin intervención humana o posibilidad de reclamación previa del jugador, determinadas sanciones que supongan la expulsión de la partida o del perfil del jugador. No se considera un argumento justificativo completo, pero sí debería tenerse en cuenta que la inmediatez en la expulsión de la partida puede estar justificada en casos concretos. En el apartado de propuestas de mejora, se expondrá la limitación a este respecto que se considera adecuada para su ponderación;

- **Derecho de oposición:** por los elementos comentados en el apartado de consentimiento sobre la existencia de advertencias específicas de que la desactivación permitida no sería real, se considera que podría existir problemática a la hora de poder determinar que se da un derecho real de oposición al propio tratamiento. Aunque no son el mismo derecho ni aplican sobre la misma base de legitimación se considera que un núcleo de naturaleza y consecuencias similares.

  Asimismo, partiendo de que no se trataría de uno de los supuestos incondicionales de mercadotecnia directa del artículo 21.2 del RGPD, sólo podría denegarse el propio ejercicio si se demostrara la existencia de un interés legítimo imperioso. En el presente caso, podría no ser justificable por no concurrir la «*esencialidad*» requerida por esta excepción[55].

  En aplicación del principio de responsabilidad proactiva, y como recomienda el EDPB en las referidas directrices sobre interés legítimo, en casos de equilibrio complicado, es recomendable establecer «*un mecanismo de exclusión voluntaria viable y bien diseñado*» para poder argumentar la disposición de una garantía adecuada al caso[56].

  Sólo en el marco de la posible denuncia por otros jugadores, aplicando por analogía lo dispuesto en la normativa de protección del denunciante, podría considerarse un

[54] Supuestos mencionados en las preguntas frecuentes de este sistema, así como en informes periódicos de actualización que el responsable emite con carácter informativo general en cada cambio de «temporada» anual. Por ejemplo: «*Informe del progreso de RICOCHET Anti-Cheat – Actualización de la Temporada 3 de Call of Duty®: Modern Warfare® II y Warzone™ 2.0*», de 4 de abril de 2023.

[55] Las «*Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679*», Adoptadas el 25 de mayo de 2018, en relación con la misma referencia al interés legítimo imperioso aplicada a transferencias internacionales, matizan con un ejemplo la existencia de un interés legítimo imperioso: «*proteger a su organización o a determinados sistemas frente a un grave perjuicio inmediato o a una sanción grave que afectaría gravemente a su empresa*.» Párrafos 5º y 6º (penúltimo y último párrafo), pág. 16.

[56] 3.6, apartado b, 2º párrafo, pág. 53.

supuesto de un interés legítimo imperioso[57] que exigiera seguir tratando dichos datos en el marco de la misma; y

- **Posible conflicto con las excepciones del 22:** al realizarse el tratamiento de prevención de trampas de manera completamente automatizada, sin intervención humana e implicando consecuencias jurídicas para el infractor; se considera de aplicación lo dispuesto en el artículo 22 del RGPD. En el apartado 2.2.6. se analizará la problemática que pudiera existir en las excepciones previstas en el precepto para levantar la prohibición inicial al respecto.

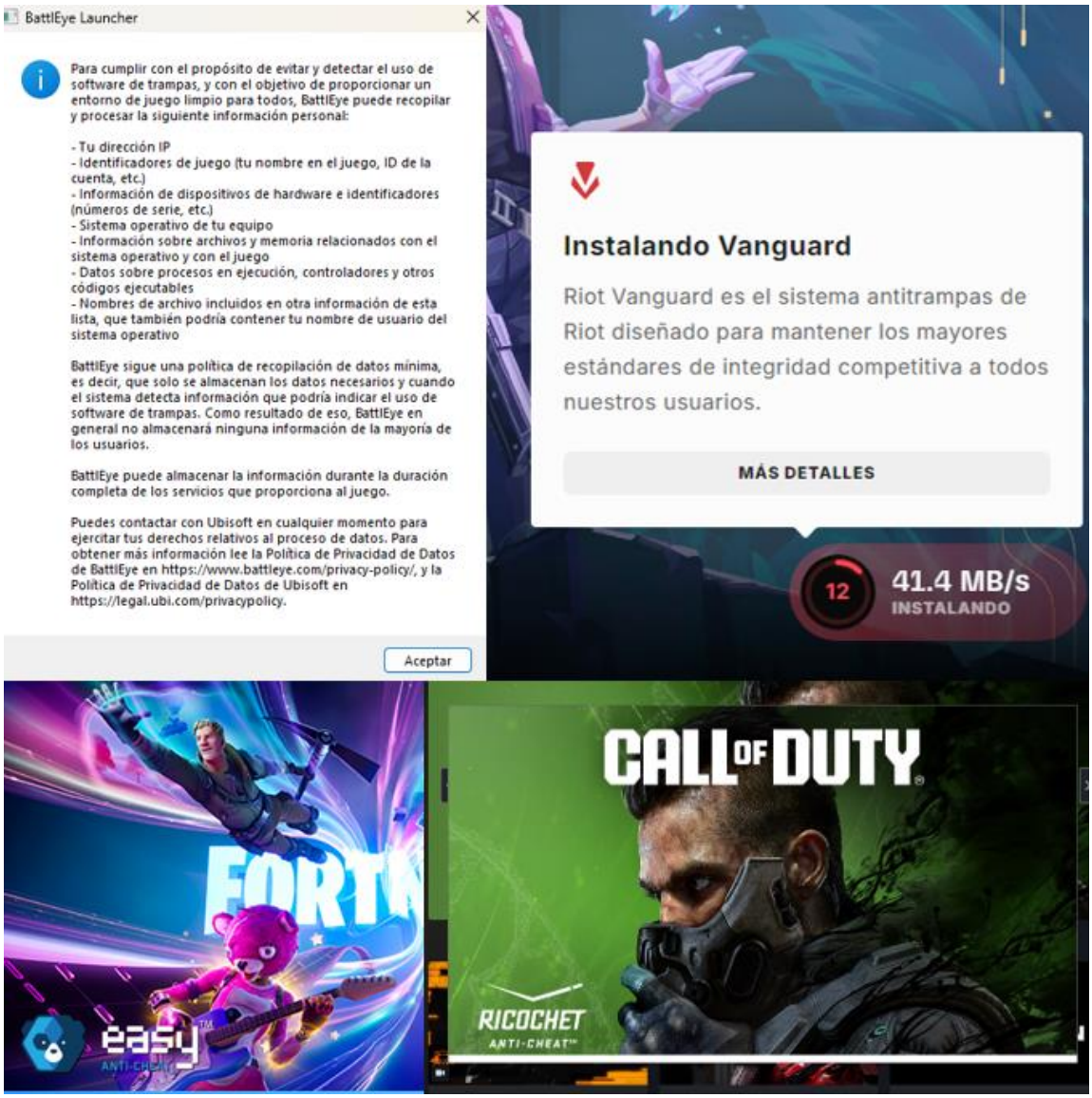


Figura 4. Combinación de capturas que ilustran el elemento comentado de que la información al jugador en el momento previo al tratamiento de datos sólo se hace de manera más concreta en el caso de BattlEye (arriba-izquierda), aunque sin llegar a ser una información de 1ª capa. En el resto de casos, se va desde la indicación de instalación del programa, hasta la aparición de la marca comercial del sistema para indicarlo.

[57] Supuesto concreto de denegación expuesto en el artículo 31.4 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

2.2.3. Destinatarios, transferencias internacionales y plazos de conservación

Se comentan de manera conjunta estos tres temas con entidad propia, por no existir información suficiente a disposición del jugador que amerite un comentario separado y en profundidad[58].

Destinatarios y transferencias

Bajo denominativos tales como; «*uso compartido de la información*» o «*a quién damos acceso a su información*», se informa de manera más o menos detallada del conjunto de cesiones que se realizarían de los datos personales tratados.

En ninguno de los casos se sigue una estructura expositiva que asocie a cada tratamiento todos los elementos de información suficiente para mostrar un contexto suficientemente concreto en cada caso. Por ejemplo, por cada tratamiento no se establece un apartado que reúna su finalidad, su legitimación, sus categorías de datos tratados, sus cesiones, sus posibles transferencias y sus plazos de conservación[59].

De conformidad a lo dispuesto por los artículos 13 y 14 del RGPD, así como en las directrices del EDPB sobre transparencia ya citadas sobre qué información concreta se debe suministrar, cabría comentar lo siguiente:

- **Categorías de destinatarios**: En todos los casos se dispone suficiente información sobre las distintas tipologías de destinatarios que pueden existir de manera habitual: intragrupo, a proveedores o a autoridades en casos concretos de necesidad; pero, teniendo también en cuenta las especialidades de posible información a los estudios de desarrollo del juego de elementos de la partida como: «*historial de partidas, estadísticas del juego o determinados elementos de la cuenta*», los necesarios si se inicia sesión a través de la cuenta de servicio de Google, Facebook y otros proveedores, o la referencia del hecho de que otros usuarios podrán acceder a la información del perfil pública o de mensajes publicados en abierto.

  Sí se advierten determinados elementos ambiguos de información en algunos de los destinatarios. Por ejemplo, que dichos desarrolladores se les puede dar «*otros datos colectivos o anónimos*», sin que se aclare quién son los primeros, si en el 2º caso se refiere por error a información no personal, o si hablan de información anonimizada sin más aclaración;

- **Concreción suficiente de los destinatarios**: en ninguno de los casos se detalla en el propio texto, o a través de ningún desplegable que pudiera encontrarse plegado al inicio, información concreta sobre la identidad de cada segmento de destinatarios, ni la indicación de lo que recomienda el EDPB en sus directrices de transparencia: «*Si los responsables optan por facilitar las categorías de destinatarios, la información debe ser tan específica como sea posible, indicando el tipo de*

[58] Asimismo, el apartado de destinatarios y de transferencias internacionales son dos materias que se entrelazan de tal manera que se suelen tratan conjuntamente para intentar garantizar la comprensión completa del tema.

[59] A tenor literal del RGPD y lo dispuesto por distintas autoridades en guías, directrices y documento de apoyo, no sería obligatoria establecer esta configuración. No obstante, se considera, que, en aplicación del principio de responsabilidad proactiva y de transparencia, facilitaría la comprensión integral de cada tratamiento llevado a cabo. Asimismo, siguiendo la pauta establecida por la propia AEPD en su Procedimiento Sancionador nº 00070/2019 sobre la entidad BBVA, en relación a mejoras en nivel de concreción de la información y el incluir de manera lo más concretamente posible los datos personales tratados en cada caso (*especialmente, en casos de consentimiento*).

destinatario (es decir, en referencia a las actividades que este ejerce), la industria, el sector y el subsector y la ubicación de los destinatarios[60]».

Solamente en los casos de Activision y de Riot se da indicación concreta de las filiales y empresas del Grupo, aunque con el elemento faltante ya estandarizado de poder consultar un listado actualizable de los proveedores que tratan datos personales.

- **Referencia a transferencias y garantías:** en ningún de los casos se concreta de manera específica los países a los que se van a transferir los datos personales en cada caso, ni más garantías que la general de que se suscribirían unas cláusulas contractuales tipo, de conformidad al modelo actual de junio de 2021 de la Comisión Europea. No obstante, tampoco se acompaña en ningún caso, de la referencia exigida en el artículo 13 y 14 del RGPD de concretar el precepto que estipula el mecanismo elegido;

- **Países con garantías**: se considera que debería existir la previsión concreta de la transferencia a Estados Unidos, por cuanto en los casos de Valve, Riot y Activision se van a transferir, o a ser accedidos, desde la matriz sita en dicho país. Solamente en el caso específico de Valve se reconoce la adhesión al marco «*Data Privacy Framework Program*» o «*DPF*»[61] sin concretar más allá de ese hecho. Asimismo, no se haría referencia a si existirían transferencias sucesivas no cubiertas por el marco de la decisión de adecuación con Estados Unidos;

- **Terceros países sin garantías:** se hace referencia general a determinados terceros países con filiales o proveedores externos que poseen una doble problemática. Son países fuera del listado establecido de estados con decisión de adecuación en vigor, y que forman parte del grupo de países con normativa problemática en materia de control o petición de información por parte de sus autoridades nacionales: «*Rusia*[62] y *Turquía*[63]». En dichos casos, no sólo sería suficiente la suscripción de unas cláusulas contractuales tipo, sino el añadido de garantías específicas al respecto y la realización de una evaluación de impacto de transferencia o «*TIA*», por sus siglas en inglés. O en caso de considerarlo adecuado, optar por las excepciones del artículo 49.1 del RGPD, especialmente del consentimiento explícito del interesado por no concurrir la pauta de ocasionalidad y repetitividad[64]; y

- **No aportación de enlace de consulta al mecanismo**: en el caso de Ubisoft y de Riot se da un enlace directo a página de consulta sobre cláusulas contractuales tipo de la Comisión Europa, pero se considera que el punto que el EDPB estipula en las referidas directrices de transparencia[65], sólo se cumpliría sí se da un enlace de

---

[60] Casilla de detalle del apartado de «*Destinatarios*» del anexo «*Información que ha de facilitarse a los interesados conforme a los artículos 13 o 14*», pág. 43.
[61] Decisión de 10 de julio de 2023 de la Comisión Europea.
[62] Analizada en el sentido de destacar la problemática en este punto, junto a la normativa específica de la India y China, en el documento encargado al respecto por el EDPS: «*Government access to data in third countries Final Report EDPS/2019/02-13*»
[63] Analizada en un 2º documento encargado, junto con la normativa de Brasil y México: «*Government access to data in third countries II Final Report Specific Contract No. 2022-0716 Implementing the Framework Contract EDPS/2019/02*»
[64] El RGPD, en su Considerando 111, estipula la aplicación de dichas pautas a la «*ejecución de un contrato*» o la «*defensa de reclamaciones*», pero no a las restantes excepciones basadas en un «*consentimiento explícito*», en «*razones importantes de interés público*», en «*intereses vitales*» y en la realización a partir de un «registro público».
[65] Casilla de detalle del apartado de «*Transferencias*» del anexo «*Información que ha de facilitarse a los interesados conforme a los artículos 13 o 14*», pág 43.

consulta al propio documento firmado, o de consulta del contenido de la decisión de adecuación concreta a la que se refiera en cada caso.

Conservación

En ninguno de los casos analizados se opta por informar de plazos de tiempo concretos, sino que varían desde la información genérica sin mayor concreción, al intento de establecer las pautas de conservación que los artículos 13 y 14 del RGPD estipulan como mínimo a este respecto.

- **Uso de generalidades:** en la mayoría de casos se utilizan expresiones desaconsejadas por no dar información real al jugador, como: «*Solo almacenaremos su información tanto tiempo como sea necesario para cumplir con los fines para los cuales dicha información se recopiló y procesó*», «*durante el periodo de retención y almacenamiento requerido por la ley*», o «*no se pueden eliminar por completo con el fin de garantizar la coherencia de la experiencia de juego o el Mercado de la comunidad*»;

- **Especificidad de los plazos:** sólo en los supuestos de Ubisoft y de Riot se particulariza la finalidad concreta de prevención de trampas e imposición de sanciones por su comisión;

- **Pautado de los plazos**: sólo en el caso de Riot se da un detalle suficiente de los diferentes escenarios de conservación por categorías de tratamiento y de la concreción de plazos de tiempo sobre posibles denuncias, tal y como indica el siguiente fragmento extraído de su política de privacidad:

  «Los factores que tenemos en cuenta para determinar estos períodos incluyen el período de retención necesario mínimo que prescribe la ley o se recomienda como óptimo, el período durante el cual se puede presentar una queja en relación con un contrato u otro asunto y si la información personal se ha agregado o seudonimizado, entre otros criterios pertinentes.

  Por ejemplo, el período de retención aplicable a sus datos personales necesario para prestarle el Servicio de Riot (por ejemplo, para acceder a los juegos) está limitado a la vigencia de su cuenta. Si se elimina la cuenta, Riot eliminará la información relacionada con este fin (prestarle el servicio), pero conservará algunos datos personales vinculados a la cuenta (como el nombre de invocador o el id. de Riot) para otros fines definidos, como la seguridad y la detección de fraudes.

  Como un ejemplo más, los datos del historial o los registros de comunicaciones se conservan al menos durante un periodo de tiempo suficiente para permitir que se presenten quejas después de una partida y, si se presenta una queja, durante un periodo de hasta dos años a partir de su creación o un periodo de tiempo suficiente para investigarla. Se guardan para permitir que Riot investigue debidamente las infracciones de sus reglas y políticas, como el fraude, las trampas y el comportamiento disruptivo.»

2.2.4. Perfilado y decisión totalmente automatizada con efectos jurídicos o significativamente similares

Como gran parte de los tratamientos realizadas por grandes proveedores de servicios digitales, se realiza en condiciones de automatización completa que permita que el servicio funcione en las condiciones ofertadas.

En esta categoría de tratamientos especialmente restringidos, estarían otros fuera de valoración, como el perfilado con el fin estricto de otorgamiento de logros por acciones predeterminada en juego, el específico para obtener información que permita entender

las actuaciones de los jugadores para poder ajustar futuros contenidos o modificaciones, o el consabido perfilado con fines comerciales.

Cumplimiento de los requisitos del supuesto

En virtud de los dispuesto en el artículo 22 y las directrices sobre esta cuestión del EDPB[66], se considera que el tratamiento de prevención de trampas reúne los requisitos de este artículo por los siguientes elementos:

- **Elaboración de un perfil del jugador:** el escaneo del dispositivo y la monitorización del jugador en partida se realizan con el objetivo de extraer conclusiones concretas y evaluar si se ha realizado alguna conducta prohibida, es decir, de su comportamiento presente[67]. Todo ello asociado y registrado en el perfil de usuario de cada jugador para la imposición de la sanciones previstas y posterior reclamación[68];

- **Existencia de una decisión sobre el jugador:** el hecho de que el propio sistema antitrampas aplique de manera totalmente automatizada la sanción prevista por la infracción detectada y validada algorítmicamente;

- **Realizada por medios totalmente automatizados y sin intervención humana:** todo el sistema se realiza sin ningún tipo de intervención humana ni tampoco significativa, determinante[69] o con validación o control alguno que permitiera eludir este requisito. Solamente se reconoce la existencia de intervención humana en la fase posterior de reclamación tras la aplicación de la sanción que hubiera iniciado el presunto infractor; y

- **Que provoca efectos jurídicos en el jugador:** se considera que cumple con este requisito, al implicar la pérdida de acceso temporal o total al servicio y contenido contratado con el responsable del tratamiento, en base al contrato y las reglas asumidas y aceptadas por el jugador. Al considerar que sí tiene esta consecuencia jurídica directa, sería innecesario realizar el comentario de si, cumulativamente, implicaría un efecto significativamente similar al jurídico.

Posible excepción habilitante

Aprovechando la valoración realizada sobre el consentimiento y la ejecución del contrato comentada en el apartado 2.2.2 de finalidades y bases de legitimación, se considera adecuado centrar el comentario en la única de las tres excepciones del artículo 22.2 del RGPD que puede ser aplicación: «*está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.»*

[66] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, Adoptadas el 3 de octubre de 2017, Revisadas por última vez y adoptadas el 6 de febrero de 2018.
[67] Uno de los ejemplos concretos que el EDPB establece como claro ejemplo de perfilado en las referidas directrices.
[68] En casos como el de la plataforma Steam (*Valve*), con indicación visual de si la cuenta de jugador está sujeta a alguna restricción por dicha razón.
[69] Matizado por el propio EDPB en las referidas directrices de decisiones automatizadas. Asimismo, con el elemento de que la decisión deba ser realizar por una persona con competencia y autoridad suficiente para ello. 4º párrafo, pág. 23.

Esta excepción no se configura de manera estricta como la base de la obligación legal que impone que el tratamiento esté completamente previsto y desarrollado[70], pero necesita contar con amparo suficiente en una norma, así como con la existencia de previsión de medidas de garantías y de equilibro sobre el interés legítimo del interesado.

Podría considerarse que los sistemas de DRM mencionados al inicio del estudio, estuvieran amparados en esta excepción por lo previsto en los artículos 196, 197 y 198 de la Ley de Propiedad Intelectual[71], en relación a las denominadas «*medidas tecnológicas de protección».*

En el caso concreto de los sistemas antitrampas objeto de análisis, podría intentar argumentarse la justificación de esta excepción por la vía de la Ley de seguridad de las redes y sistemas de información[72] y su artículo 16, que determina que los prestadores de servicios digitales[73] deberán adoptar las medidas técnicas y de organización, adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de sus servicios[74]. No obstante, se consideran los siguientes elementos de problemática de esta interpretación:

- Sólo aquellos actos considerados trampas, que, necesariamente, afecten a la seguridad y funcionamiento estricto del juego, podrían considerarse amparados por esta norma. La fase previa de escaneo del dispositivo y el comportamiento del jugador, aun cuando supone una alteración del equilibro y condiciones de la partida, se considerarse que no podría interpretarse como estrictamente de «*seguridad de las redes y sistemas de información*».

- Dicha norma podría considerarse que no incluiría medidas y salvaguardas concretas para garantizar los derechos e intereses de los jugadores.

Derecho a intervención humana y a impugnar la decisión

Como derechos ineludibles que se deben permitir a los jugadores, estaría la posibilidad de exigir intervención humana o poder impugnar o reclamar la decisión. En todos los casos analizados, se cumpliría con estos parámetros en el marco de la posibilidad de reclamación posterior y revisión frente a sanciones aplicadas que se considere injustas.

En el apartado 2.4., relativo la posibilidad de denuncias de otros jugadores, se concretará el funcionamiento general del sistema. Se adelanta que la revisión por equipo especializado no se realizaría hasta la posible reclamación por infractor sancionado, es

[70] Junto con la matización que el artículo 8.1 de la LOPDgdd determina sobre la necesidad de esta previsto en norma con rango de ley. En la reciente resolución del TJUE (*asuntos acumulados C-17/22 y C-18/22*), de 12 de septiembre, se considera la interpretación de que la jurisprudencia (*se entiende que en España se referiría en exclusiva a la emitida por el Tribunal Supremo*) cabría en el marco de la obligación legal, aun cuándo se deja la cuestión abierta a que a nivel nacional que compruebe que sea clara, precisa y suficientemente garantista en cada caso

[71] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

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

[73] 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 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».*

[74] 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*».

decir, en los mismos términos que no permitirían justificar realmente que exista una intervención humana dirimente como se ha comentado.

Información

Relacionado con el apartado anterior de que sin información clara no podrá ejercerse en términos adecuados los derechos a intervención humana e impugnación[75], así como del elemento principal de dar indicación al jugador suficiente del funcionamiento del sistema, su relevancia sobre el jugador y las consecuencias previstas (*información significativa del mismo*), cabe determinar lo siguiente:

- **No indicación de perfilado y decisión del 22**: Valve y Ubisoft no indican referencia alguna en sus respectivas políticas de privacidad que pueda permitir valorar el nivel de cumplimiento de la información;

- **Negación completa**: Activision niega completamente la existencia de perfilado y decisiones automatizadas del artículo 22, sin dar indicaciones suficientes en ninguna información para corroborar si todo el sistema tiene intervención significativa o no: «*No practicamos la «elaboración de perfiles» para promover decisiones que produzcan efectos legales o de importancia similar*».

- **Información adecuada:** Riot incluye en apartado específico de su política de privacidad una descripción que se considera suficientemente explicativa para cumplir con la información este punto. Se consideraría necesario incorporar una 1º capa informativa mostrada al jugador para asegurar el deber de información, así como hacer mención expresa a la 1ª fase de escaneo del dispositivo realizada fuera de los «*Servicios de Riot*».

  «E. Sistemas antitrampas y prevención de fraude

  Para poder supervisar el cumplimiento de nuestras políticas antitrampas y de prevención de fraude, desarrollamos plantillas de patrones de comportamiento inadecuado (por ejemplo, trampas o fraude), que consideramos indicativos de comportamientos prohibidos. Para ello, nos basamos en un análisis de comportamientos reales en los Servicios de Riot.

  Estos patrones de comportamiento inadecuado se clasifican en función de su gravedad con distintas consecuencias (por ejemplo, restricciones de cuenta temporales o permanentes, restricciones de comunicación, eliminación de contenido o acceso limitado al contenido de los juegos) para los jugadores según la transcendencia de su conducta. Nuestras herramientas automatizadas utilizan estos patrones de comportamiento inadecuado y sistema de clasificación para compararlos con su comportamiento a lo largo del tiempo y, si se determina que su comportamiento es inadecuado, para tomar una decisión sobre las consecuencias que este tendrá para usted. Principalmente, esto nos permite aplicar nuestras reglas y políticas, proteger los Servicios de Riot, detectar e impedir actividades no autorizadas y mantener la integridad competitiva de nuestros juegos.

  Nuestro procedimiento de quejas puede permitirle recurrir una decisión. En este caso, puede solicitar que uno de nuestros agentes revise su caso. Este tomará una determinación final manual sobre el resultado correcto en función de las pruebas disponibles.»

[75] Elemento recordado por el EDPB en las directrices sobre decisiones automatizadas, último párrafo, pág 30.

2.2.5. Evaluación de impacto

El presente tratamiento de prevención de trampas, exigiría dicha evaluación de impacto por reunir múltiples de los criterios que determinan el artículo 35.3 del RGPD y el listado de supuestos realizado por la AEPD[76].

Supuestos aplicables

Del artículo 35.3 del RGPD, respondería al primer supuesto del apartado a):

- «*Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar*»;

Del propio listado de la AEPD, y por todo lo expuesto anteriormente, reuniría los siguientes 7 supuestos[77]:

- *1*[78]. «*Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.»* Por cuanto realiza un análisis del comportamiento del jugador para determina si realizar trampas, así como lo asigna al perfil de jugador preexistente;

- *2. «Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.»* Por cuanto es el propio algoritmo del sistema antitrampas el que aplica de manera automática la sanción ante la detección del posible acto;

- *3. «Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.»* Por el hecho de que observa en tiempo real al jugador para obtener información técnica y personal que permita al algoritmo detectar conductas sancionables, sobre un usuario concreto y un dispositivo concreto asignado a él;

- *7. «Tratamientos que impliquen el uso de datos a gran escala.».* Por el hecho de que se realiza un tratamiento a nivel global de todos los jugadores, generalmente segregados por servidores de varias regiones mundiales: Asia, Europa, Estados Unidos o Sudamérica, entre otros;

- *9. «Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y*

[76] Competencia conferida por el apartado 4 del propio artículo 35. Relación de supuestos de «*Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4 del RGPD)*».

[77] Partiendo de la pauta dada en el referido listado de que se deben reunir como mínimo dos criterios de manera simultánea.

[78] Se mantiene la numeración original de cada criterio establecida en el listado.

víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.» Por el hecho de que en los videojuegos objeto de estudio existe un número indeterminado de jugadores menores de catorce años. Especialmente, en juegos como Fornite que se enfocan y ofrecen con edad recomendada y mínima de 12 años[79].

- *10. «Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.»* Por el hecho de utilizar un sistema algorítmico con una tecnología de mercado, pero de una manera suficientemente intensa y a escala como para considerar que existe un riesgo propio en este sentido; y

- *11. «Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD».* En el sentido de que el tratamiento objeto de estudio está destinado a inhabilitar o denegar el acceso de los jugadores al servicio que han contratado, por el efecto ya comentado de retirada de acceso por sanción, o no apertura y carga del juego por error y conflicto con otros programas[80].

No se considera como supuesto de aplicación el punto del apartado 11 del listado sobre el impedimento de ejercicio de derechos, por cuanto el artículo 15.4 del RGPD establece una excepción posible a la satisfacción de derecho de acceso. En el apartado 2.2.6 se expondrá la posible problemática entra la excepción y la denegación indebida del ejercicio de este derecho en el caso concreto.

El artículo 35.7 del RGPD determina los siguientes elementos que debe reunir, valorar y conseguir garantizar suficientemente la evaluación de impacto. Sin ánimo de reiterar argumentación precedente sobre la necesidad, proporcionalidad, legítimas expectativas o efectividad real de los sistemas antitrampas, solamente se procederá a completar el conjunto de elementos que deberían tenerse en cuenta.

Al igual que en el apartado sobre interés legítimo, no se dispone de acceso o información suficiente detallada como para proceder a realizar un comentario profundo del mismo.

- **Evaluación de riesgos:** la realización que todo tratamiento exige de ponderación previa de las amenazas y riesgos existentes[81];

[79] Sancionado, en diciembre de 2022, por la Comisión Federal de Comercio Estadounidense (*FTC, por sus siglas en inglés*) con doble multa de 275 millones de dólares por falta del consentimiento de los padres o tutores legales y la aplicación de parámetros por defecto perjudícales para los menores; y por la imposición de devolución de 240 millones por utilizar sistemas de patrones oscuros y técnicas engañosas para incentivar las compras dentro del juego.
[80] Se considera de relevancia citar el ejemplo similar que el EDPB da sobre este supuesto, en sus «*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*», 3º párrafo, apartado 9, pág. 12.
[81] La AEPD en la referida guía de evaluación de análisis de riesgos y evaluación de impacto, determina que el análisis de riesgos y la evaluación de impacto no son elementos aislados, sino que la evaluación de impacto es un elemento que forma parte del proceso de gestión de riesgos, Apartado, II, J,.1 y .2, págs. 25 y 26.

- **Medidas de seguridad implantadas:** en relación con el punto anterior, y la exigencia del artículo 32 del RGPD, la delimitación de las medidas concretas que se plantean para conseguir garantizar la seguridad del tratamiento. Asimismo, los límites y restricciones establecidos en el tratamiento para minimizar posibles daños o efectos indeseados; y

- **Consulta a los interesados o partes interesadas (*«stakeholders»*):** al establecer este elemento como opcional y a discreción del responsable si se considera procedente, se suele argumentar que no es necesario casi en ningún caso[82]. En el presente supuesto de un riesgo alto con un acceso total al dispositivo, se considera que debería ser imprescindible recabar la opinión y valoración previa de grupos de interesados y de entidades representativas[83].

Riesgos sobre la aplicación a menores

Como elemento de valoración adicional, existiría el punto de la aplicación de este tratamiento de prevención de trampas a todo jugador menor de edad que acceda al mismo. El enfoque en el segmento de menores de 12 años para intentar abarcar al mayor número de jugadores posibles, así como el hecho de que gran parte de sus referentes sean creadores de contenido ligados al sector de los videojuegos, hacen que los menores de edad sean uno de los segmentos que más juegan en videojuegos de ámbito multijugador. Esto implicaría tener en cuenta, al menos, los siguientes límites y elementos de valoración concretos, como los siguientes:

- **Tratamiento del artículo 22 del RGPD:** este precepto no realiza una distinción entre el tratamiento de mayores o menores de edad, pero los Considerandos 71 y 75 establecen la pauta de que no se deberá aplicar un tratamiento de elaboración de perfiles totalmente automatizados y con efectos jurídicos o significativamente similares sobre menores. Este no constituye una prohibición absoluta al no haberse establecido como tal en el propio articulado del RGPD, pero sí debería actuar como un elemento limitativo objeto de justificación o exclusión para menores[84].

- **Información adecuada al menor:** sólo en el caso analizado de Epic se hace mención concreta a información relativa a menores, pero no responde al hecho de estar redactada ni adaptada para facilitar su comprensión. Únicamente, es una explicación breve para los padres o tutores legales del menor.

  Un ejemplo de la extendida costumbre de responsabilización completa de los padres y tutores legales, sin que el responsable asuma en 1ª persona la obligación de redactar una información totalmente adaptada a la horquilla de edad de los menores que la etiqueta de edad recomendada del juego

[82] Asimismo, por el hecho de que debe ser una consulta real y pormenorizada sobre los factores de riesgos y su incidencia, y no una mera encuesta o documento formal.
[83] A este respecto, sería interesante interpretar el concepto de manera amplia para recabar la opinión especializada de entidades de representación que incluyan como asociados principales a los posibles interesados afectados: asociaciones y entidades de defensa de usuarios, internautas o jugadores.
[84] De conformidad a lo dispuesto por el EDPB en sus directrices sobre decisiones automatizadas, podría entenderse justificada la aplicación sobre menores si el fin es proteger su bienestar. En el caso concreto de estudio, sería complicado poder justificarlo en dichos términos. Apartado V, pág. 31.

establezca[85] [86]. Esto implica no sólo el riesgo de incumplimiento en materia de información de los artículos 13 y 14 (*junto con lo establecido por el Considerando 58*), sino que el menor no sea consciente realmente del funcionamiento de algo que por edad no tiene tan interiorizado ni puede entender como un adulto;

- **Sistema de comprobación de edad y limitaciones:** en ninguna de las plataformas y perfiles de usuario en las que se incluyen los juegos y sistemas antitrampas objeto de estudio, se dispone de un sistema de comprobación de edad efectivo, o que se encuentre en proceso de adaptación a las pautas o propuestas que se han ido presentado en el marco del proceso de regulación de menores que se están promoviendo en España[87].

  Todas las plataformas se enfocan en establecer una cuenta de menor de edad y otra cuenta de mayor de edad que tutele la primera, y que permita activar las funcionalidades restringidas de compra o chat. En algunos casos, no se permite de base introducir nombre real, pero se basa en un sistema de introducción de edad fácilmente eludible si el menor incluye una edad superior al de mayoría legal. Asimismo, dichas restricciones mencionadas, no aplicarían al preste objeto de estudio de limitar, desactivar o no aplicar los sistemas antitrampas y el escaneo completo del dispositivo.

  Asimismo, el riesgo legal inherente en la interpretación de que la responsabilidad única es de los tutores legales o padre, pero no de propio responsable del tratamiento. Enunciado con expresiones ¡, tales como las que utiliza Ubisoft en sus condiciones de uso: «*En la medida en que la ley lo permita, denegamos toda responsabilidad derivada de actividades que pudieran realizar usuarios menores de edad sin el permiso de sus padres o tutores legales. En todos los casos, todo uso de los servicios por parte de usuarios menores será responsabilidad de sus padres o tutores legales*».

- **Interés superior del menor:** el gran principio que rige en toda la normativa para otorgar una protección más elevada para los menores[88], y, que, puede encontrar su amparo en el RGPD en su Considerando 38. Como potenciales riesgos concretos que deberían valorarse, cabría destacar los siguientes del listado del Instituto Nacional de Ciberseguridad (*INCIBE*) que recoge la AEPD en su nota

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

[86] La ley «*California Age-Appropriate Design Code Act (CAADCA)*», anulada en septiembre de 2023 y en proceso de recurso de apelación, planteaba completar las restricciones impuestas por la COPPA con otras de interés: restricción de recopilación de datos innecesarios y perfilado, obligación de entregar a la Fiscalía General las evaluaciones de impacto realizadas en un plazo máximo de 3 días desde la petición, sistemas razonables de verificación de edad o la propia información adaptada y específica para menores.

[87] El decálogo de principios y prueba de concepto que la AEPD presentó el 14 de diciembre de 2023, o la reciente presentación en julio de 2024 de la aplicación de verificación de edad para acceso a sitios de contenido pornográfico, denominada «*Cartera Digital Beta*», dentro del marco de regulación vía «*Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales*».

[88] No se define en la normativa nacional o internacional específica (*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*), pero podría conceptualizarse como «*mantener el bienestar del menor de la manera más amplia posible, especialmente en los ámbitos de la seguridad, salud, bienestar, relaciones familiares, desarrollo físico, psicológico y emocional, identidad, libertad de expresión y privacida*d».

técnica: «*Protección del menor en Internet – Evita el contenido inapropiado preservando su privacidad*».

- **Daños psicológicos, emocionales y sobre la salud física:** como consecuencia de no entender la causa del funcionamiento inadecuado del juego si existe algún fallo de configuración, o verse obligado a decidir autorizar o aceptar todo lo que el sistema exige sin posibilidad real de negativa. Asimismo, por la presión de consumo irreflexivo del sistema usual de micropagos, recompensas diarias si se accede, o por no verse excluidos del juego de moda en su entorno de amistades;
- **Desinformación, manipulación y construcción de falsas creencias:** como consecuencia de no recibir una información adecuada que le induzca a pensar que no tiene un verdadero derecho a la protección de datos ni a decidir nada relacionado con sus datos personales;
- **Inclusión en grupos y colectivos dañinos, o realización de conductas peligrosas o socialmente inapropiadas:** el hecho de permitir el acceso a las herramientas propias de comunicación en partida y la propia plataforma. Se ha indicado que existe limitación pensada para menores, pero sujeta al sistema incompleto de comprobación que provoca que los menores se vean expuestos, o participen activamente en la multitud de conductas tóxicas e inapropiadas realizas en este tipo de chats. En el apartado de grabación de chats de voz, se expondrá la posibilidad alternativa y menos invasiva para este tipo de funcionalidades.

Breve referencia al DPD

Se considera relevante mencionar la obligación de contar en cada caso analizado con un delegado de protección de datos. Se incorpora en este apartado por dos razones principales: se considera que no tiene la entidad suficiente para hacerlo de manera separado, y por existir el nexo causal de que el delegado de protección de datos en entidades que deban tenerlo, deberá asesorar en materia de evaluación de impacto a su responsable (*artículo 35.2 del RGPD*).

Se considera dicha obligación de nombramiento para cada uno de las entidades detrás de los sistemas objeto de estudio, por encontrarse dentro del supuesto del artículo 37.1.b del RGPD:

- **Actividad principal**: la actividad principal de cada responsable implica tratar datos de manera habitual y nuclear. No sería posible establecer un sistema antitrampas sin el tratamiento y análisis de información, ni tampoco dar un servicio de juego multijugador sin gestionar la información personal necesaria para emparejar, asignar el servidor más adecuado o mantener la partida. Eliminado el componente de tratamiento de datos de categoría especial que implica la gestión del gran ejemplo de un hospital que se pone en esta materia, se considera que el presente caso supone un tratamiento al mismo nivel de necesidad de dato personal para la gestión ordinaria de la actividad;

- **Observación habitual y sistemática:** por ser consustancial al tratamiento pretendido. Asimismo, por responder a la interpretación que el EDPB da en las referidas directrices sobre dichos conceptos: «*habitual*» como: «*que tiene lugar de manera constante o periódica*»; y «*sistemátic*o» como: «*que tiene lugar como parte de un plan general de recogida de datos*» o «*preestablecido, organizado o metódico»; y*

- **Gran escala**: el tratamiento se entiende que alcanzaría esta categoría por el número de millones de jugadores a nivel mundial de cada título, por volumen de información personal que se debe gestionar para su funcionamiento, por el alcance geográfica mundial y por la intensidad del análisis tiempo real del dispositivo y la conducta del jugador.

Dicho lo anterior, en los casos de VAC y de BattlEye no se declara la existencia del mismo, ni de ninguna dirección de contacto específica que no sea le general de protección de datos. Asimismo, en ninguno de los casos objeto de estudio se constata su comunicación a nivel de registro de delegados de la AEPD, de conformidad al artículo 34.3 de la LOPDgdd.

Aunque todas las grandes editoras tienen filiales en prácticamente todos los países, incluyendo España[89], sólo un reducido grupo de entidades se ha registros a nivel de España. Por ejemplo: NINTENDO IBÉRICA, S.A.U, WARNER BROS. ENTERTAINMENT105 o SONY INTERACTIVE ENTERTAINMENT ESPAÑA S.A.

2.2.6. Derecho de acceso

En atención a la materia tratada, se va a proceder a centrar exclusivamente el comentario sobre derechos en el relativo al acceso. Se considera que el resto de derechos recogidos en los artículos 15 a 22 son de relevancia capital, pero en el presente caso específico de acceso sería el que podría haber permitido confirmar los datos personales objeto del tratamiento.

Particularidades del derecho acceso en el supuesto objeto de estudio

Como se ha enunciado en el apartado 2.1. de análisis de los registros generados, en algunas de las políticas y documentos de preguntas frecuentes que informan del tratamiento y sistemática del proceso se indica, sin conceptualizarlo en términos de protección de datos, que las posibles peticiones de información específica sobre el análisis se tramitarán de manera limitada.

El derecho de acceso siempre ha suscitado dudas sobre el límite de información a aportar, o incluso si se debe cumplir con dicha obligación en casos en los que se encontrará ya debidamente bloqueada[90].

El EDPB en sus Directrices 01/2022 sobre el ejercicio del derecho de acceso, hace referencia expresa, en modo de ejemplo hipotético[91], a la actuación que debería tener el responsable de este tipo de sistemas antitrampas. En particular:

- Confirmación de que se ha decidido restringir el acceso por las trampas concretas que se aduzcan, sobre la base de los términos y condiciones o código de conducta;

[89] Actualmente, el proceso de repliegue de muchas entidades hace que se cierren muchas filiales y se centralize todo el mercado comunitario desde una única a nivel europeo. Aunque manteniendo las cuentas de redes sociales y personal en ese sentido para labor de contacto y promoción.

[90] Este tema ya ha sido resuelto por la propia AEPD en varias de sus resoluciones. Por ejemplo, la nº 00532/2020 en la que se determina que el hecho de que la información estuviera bloqueada, de conformidad al artículo 32 de la LOPDgdd, no puede suponer la denegación de la entrega de copia de la información tratada en la que consiste un derecho de acceso. 2º párrafo, pág. 4.

[91] Directrices 01/2022 sobre los derechos de los interesados —Derecho de acceso, ejemplo 37, pág 62.

- Proporcionar una copia de todos los datos personales tratados del jugador. En particular, el EDPB determina que deberá facilitarse al jugador la información específica que haya dado lugar a la decisión, a fin de que quede informado y pueda verificar su exactitud: resumen del registro, fecha y hora de la trampa, detección de software de terceros, entre otros); y

- Recordando el límite establecido el artículo 15.4[92], y más enfocado en lo interesante para el caso actual, de no tener la obligación de incluir información clave que pudiera implicar una vulneración del secreto comercial, propiedad intelectual o de cualquier otra índole.

Este límite del último punto implicaría que no se comunicará información técnica del funcionamiento del algoritmo, pero se considera que no debería suponer la negativa del responsable a incluir una referencia redactada sobre qué información analiza, si es en tiempo real, cuando está activo, si tiene acceso a nivel de administrador, si sólo accede a carpetas propia del juego concreto u otros elementos de los que sí se informa en documentación publicada fuera del cliente del juego y las políticas de privacidad. Se considera lo anterior dos razones principales:

- El hecho de dar demasiada información de corte técnico o que implique un conocimiento real puede poner en riesgo el principio de transparencia. Asimismo, mucha de esa información a nivel de usuario que permitiría comprender a bajo nivel el funcionamiento, ya se encuentra ubicada en información en preguntas, páginas webs e información en abierto accesible fuera de la plataforma de juego; y

- La excepción ponderable que el artículo 15.4 da sobre derechos de terceros, puede intentar interpretarse de manera interesada por los responsables para no dar ningún tipo de información que permita al interesado ser informado en los términos del RGPD, es decir, un incumplimiento real del RGPD.

  Este punto de interpretación problemática del 15.4, aunque opuesto al enfoque de este estudio, se ha comunicado al EDPB por las entidades de representación a nivel europeo de la industria, Interactive Software Federation of Europe (ISFE) y European Games Developer Federation (EGDF), en el momento de apertura del plazo de consulta pública. Se parte de la premisa de cualquier información concreta permitiría vulnerar el sistema y causarle un perjuicio, es decir, que debería concederse un mayor grado de discrecionalidad al responsable para poder determinar hasta dónde da información[93].

Resultado del ejercicio del derecho de acceso

A fin de poder comprobar si suministraría dicha información en un ejercicio de derecho de acceso, a excepción de la causa de cualquier trampa realizada y la subsiguiente

[92] Y con su reflejo en el Considerando 63 que determina que «*no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos*», aunque con el límite de que no pueda implicar una negativa a su satisfacción.

[93] «*Joint ISFE-EGDF Reply to the Public Consultation on the EDPB's Guidelines 01/22 on Data Subject Rights – Right of Access*». Punto 32, pág. 9 «*Aunque el ejemplo en las Directrices es útil, debería ir más allá para reconocer que los controladores tienen mayor discrecionalidad para denegar el acceso a los datos personales de los jugadores cuando se trata de sus actividades fraudulentas. Debería considerarse una medida necesaria y proporcionada*.» Asimismo, de interés los puntos 28 a 3, págs. 8 a 10.

restricción por no haber vulnerados los términos, se ha procedido a solicitar un derecho de acceso a cada uno de los cinco responsables de los sistemas analizados.

En dicho ejercicio, se ha solicitado copia concreta de los datos personales específicos que hubiera gestionado el sistema antitrampas, información significativa de la lógica y funcionamiento del algoritmo, así como la indicación de que la redacción o falta de determinada informada por lo dispuesto en el artículo 15.4, no puede implicar la desestimación del mismo de manera completa.

Pueden consultarse el texto original redactado del ejercicio de derecho y el intercambio de correos de la petición en la carpeta en nube a correspondiente, mencionada y accesible desde enlace del apartado 1.3 de metodología o en el apartado 1.4 de bibliografía. En todos los casos se da la posibilidad de ejercerlo mediante formulario específico tras autenticación en la página principal, o vía soporte interno dentro la plataforma de juego, facilitando así el trámite y evitando la solicitud de información identificativa para confirmar la identidad del solicitante.

En la respuesta al ejercicio de derecho realizado en ninguno de los casos se ha dado la información solicitada, sino que se ha remitido a la generación de un entregable centrado en datos recopilados y datos observados, pero no en los inferidos[94] o sometidos al artículo 22 de ningún modo. Las respuestas recibidas al ejercicio han sido de dos tipologías concretas:

- Remisión al sistema de generación automático de entregables con los datos personales, sin que quepa la posibilidad solicitada de recibir sólo la información pretendida, ni que el mensaje remitido por cauce adecuado sea revisado por el DPD o el departamento de protección de datos ante la peculiaridad que supone; o

- Remisión a un listado con información general del jugador en la propia plataforma de juego[95], con la advertencia concreta ya adelantada de que no van a facilitar información por riesgo de comprometer el sistema. Incluso en los casos en los que asumen de manera errónea que se ejercía como consecuencia de una restricción de juego (*el ejemplo específico dado por el EDPB*): «*Los datos de cuenta utilizados para VAC, prohibiciones de juego y factor de Confianza están diseñados para proteger a los clientes de actividades hostiles a los usuarios y no son recuperables por el usuario. Compartir esta información comprometería estos sistemas, y por esta razón no compartiremos estos datos (…..).*» o «*No podemos facilitarle información sobre su expulsión porque debemos garantizar que el juego sea justo, seguro y divertido para todos nuestros jugadores*».

En cuanto al contenido de los derechos de acceso realizado, se consideran las siguientes conclusiones:

- La no obtención de la información concreta requerida, ni de la explicación de la lógica y elementos del artículo 22 también exigidos (*estipulado en apartado 1.h de este mismo artículo 15 como parte del derecho de acceso*), aportando solamente la información de datos recopilados, accesos o historial de partidas. Se considera que no iría en consonancia con el derecho del interesado de

[94] Del tenor literal del artículo 15 de obtener «*copia de los datos tratados»* sin especificar limitación alguna, como en casos de portabilidad, y por lo especificado por el EDPB en las referidas directrices del derecho de acceso, y con mención específica a los «*resultados algorítmicos*». Punto 97, pág. 38. 3º punto de la continuación del listado.

[95] Una modalidad válida de satisfacer copia de la información por acceso a la información dentro un «sistema seguro en remoto», tal y como establece la propia EDPB en dichas directrices. Punto 186, pág. 66.

concretar a qué datos quiere acceder, así como la aportación de la máxima información redactada o limitada si se considera de aplicación la limitación del artículo 15.4 por código fuente o secreto empresarial;

Dicho enfoque de dar la máxima información sin suponer una obligación de información de cuestiones de complejidad técnica excesiva o revelación del algoritmo utilizado, se referencia por el Abogado General del TJUE en el asunto C-203/22[96]: "*Deduzco de estos elementos que el responsable del tratamiento no está obligado, en virtud del artículo 15, apartado 1, letra h), del RGPD, a facilitar al interesado información de carácter técnico que este no podría comprender, como los detalles de los algoritmos utilizados. (50) Por otro lado, el responsable del tratamiento debe cumplir su obligación de facilitar al interesado, en cada caso, información, a la vez, accesible y suficientemente completa sobre el proceso que condujo a la decisión automatizada en cuestión y sobre las razones que explican el resultado al que se llegó en dicha decisión. (…….). (51) Por tanto, el interesado debe poder comprender qué información se ha utilizado en la toma de decisión automatizada y cómo se ha tenido en cuenta y ponderado*."

- Cumplimiento adecuado de medidas de seguridad del artículo 32 del RGPD al efecto, al estar la información accesible desde la cuenta de usuario del jugador tras autenticación, o remitir copia de la información cifrada que se descomprime con programa de uso habitual y contraseña remitida por otra vía; y

- Generación de entregables que cumplen con el elemento de claridad expositiva necesario, salvo en el caso de Ubisoft que se remite copia de varios Excel exportados directamente del sistema sin leyenda explicativa.

2.3. Patrones oscuros y patrones engañosos

Siguiendo la creciente preocupación y foco de las autoridades de protección de datos por cualquier técnica o configuración que presione, condicione o engañe al interesado, generalmente, bajo los denominativos de «patrón oscuro» (*«dark pattern» en inglés*) o «patrón engañoso («*deceptive desig pattern», en inglés*); se considera su comentario aplicado al objeto de estudio

A efectos de mera concreción, se expone la definición propia basada en la conceptualización más clásica de mención al fenómeno de la psicología aplicada al marketing, o «*neuromarketing*»: «*El uso de técnicas de neuromarketing con la finalidad de que el usuario acabe haciendo/dando/comprando lo que el responsable quiere, pero sin que sea consciente de su decisión ha sido forzada o inducida*.»

En esta materia concreta, tanto el EDPB[97] como la propia AEPD[98], han emitido directrices especificas al respecto. En el caso del EDPB en un sentido más general y enfocado en todo el conjunto de patrones, mientras que las relativas a la AEPD se centran en las que tiene un componente netamente de adición: «*patrones adictivos*».

Se considera de mayor utilidad tomar como elemento de contraste exclusivo las categorías dadas por el EDPB, por su coincidencia en posibles patrones existentes en los sistemas antitrampas. Asimismo, por el hecho de que los patrones adictivos

[96] Asunto C-203/22 - Petición de decisión prejudicial planteada por el Verwaltungsgericht Wien (Tribunal Regional de lo Contencioso-Administrativo de Viena, Austria. Conclusiones presentadas el 12 de septiembre de 2024. Conclusión nº76.

[97] «*Directrices 03/2022 sobre Patrones de diseño engañosos en las interfaces y plataformas de medios sociales: cómo reconocerlos y evitarlos»,* versión 2.0, adoptadas el 14 de febrero de 2023.

[98] «*Patrones adictivos en el tratamiento de datos personales Implicaciones para la protección de datos*», de julio de 2024.

especificados por la AEPD se encontrarían en el resto de tratamiento y elementos del videojuego fuera del objeto: inducción a entrar diariamente por recompensas o fomento de la compra irreflexivas con micropagos, entre otras conductas.

Partiendo de las categorías del EDPB dadas en dichas directrices, así como toda la información y elementos de prueba de los que se dispone sobre el tratamiento objeto de estudio, se podrían existir los siguientes patrones engañosos:

- **Incitación continua, continuidad forzada o «*Continuous prompting*»:** en el sentido de recordar continuamente que se debe autorizar el acceso a nivel de administrador del sistema antitrampas, así como la obligación de desactivación de todo el conjunto de elementos que pudiera detectarse como trampas o sistemas incompatibles. Considerando que dicha actuación puede implicar una infracción del principio de limitación de finalidad o de licitud;

- **Laberinto de privacidad o «*Privacy maze*» y Descontextualización o «*Decontextualising*»:** en forma de separar información relevante sobre el alcance, funcionamiento y consecuencias entre la política de privacidad y los documentos de soporte o preguntas frecuentes accesibles por consulta externa. Asimismo, el elemento de que sólo en el caso citado, y con la captura ya referenciada, se da una 1º capa informativa que permite al jugador tener una idea general en el momento en que debería por RGPD. Considerando que dicha actuación puede implicar una infracción de los principios de transparencia, licitud y cumplimiento adecuado del deber de información;

- **Dirección emocional o «*Emotional Steering*»:** en el sentido de hacer también responsables por un fin deseado compartido a los jugadores, con expresiones como «*ayudarnos a mantener un juego seguro, limpio y divertido*». Se considera que el mecanismo alternativo de denuncia por conductas de otros jugadores del apartado siguiente respondería legítimamente por permitir al jugador hacerlo o no hacerlo, pero no así en el punto de autorización para acceso y escaneo de su dispositivo. Considerando que dicha actuación puede implicar una infracción del principio de transparencia, licitud y ejercicio de derecho de oposición (*por convencer al usuario para que nunca se intente oponer al mismo).*

  Asimismo, por el uso de expresiones que inducen a pensar que siempre existe un pleno y absoluto cumplimiento de la privacidad y protección de datos, con expresiones tales como: **«***sigue una política de minimización de datos que garantiza que los datos sólo se almacenan cuando es necesario*», «*Tu privacidad no es un juego*», o la recomendación ya comentada al inicio de hacerle ver al jugador que la recomendación de seguridad del Windows lleva a configurar a nivel de kernel;

- **Acción engañosa o «*Misleading Action*»:** en el sentido de dar la posibilidad de desactivar o desinstalar el sistema antitrampas, para luego advertir que debe volver a reactivarse si se desea cargar y hacer funcionar el propio juego. Considerando que dicha actuación puede implicar una infracción del principio de transparencia, licitud y ejercicio de derecho de oposición (*por convencer al usuario para que nunca se intente oponer al mismo*); o

- **Ajuste engañoso o «*Deceptive snugness*»:** en el apartado 2.5 relativo a la grabación de chats de voz, se realizará comentario con apoyo de capturas específicas sobre las distintas opciones de chat preactivadas por defecto. Con la posibilidad de implicar una infracción de los principios de privacidad por diseño y por defecto.

2.4. Denuncias de otros jugadores

En un momento anterior de este estudio se ha hecho mención a que la fase de denuncia de otros jugadores podría ser una de las alternativas menos invasivas a la 1ª fase de escaneo en tiempo real del dispositivo del usuario. Actualmente, se configura como una parte más del tratamiento de prevención de trampas, pero por detrás de esa primera de detección y escaneo del dispositivo configurada como prioritaria.

En un primero momento de valoración, podría argumentarse que sería parte del proceso más amplio del sistema o canal de denuncias en el ámbito empresarial que incluye a empleados, proveedores o clientes, regulado por la «*Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*»; pero no entraría en el ámbito de aplicación concreto de dicha normativa. No obstante, en el apartado 2.8 de propuestas de mejora se plantearán algunas basadas en la estructura y en lo dispone dicha normativa para generar un canal de reclamación más sólido y garantista.

2.4.1. Funcionamiento

Los sistemas de denuncias de los casos objeto de valoración, responden al siguiente esquema de fases que les dota de unas reglas suficientes ante cualquiera reclamación por vía de consumidores y usuarios[99]:

- Formulario de denuncias incluido en una sección de menú fácilmente accesible desde la partida en la que el jugador se encuentra, o a través de un desplegable que puede abrirse mediante pulsación del nombre de usuario del infractor en la lista pública y consulta de jugadores en partida;

- Selección de la conducta a denunciar: trampas, abuso de algún error en el juego, conducta antideportiva o que perjudica al equipo de jugadores del que forma parte el presunto infractor, abandono de partida que puede perjudicar el equilibrio[100], o varias opciones por comportamiento inadecuado en chats de voz;

- Indicación lo más ajustada posible del momento exacto en partida para su posterior visionado de revisión[101];

- Comprobación de manera totalmente automatiza y asignación de la sanción por el sistema sin intervención de personal humano; y

- Posibilidad de reclamación por parte del jugador infractor tras la imposición de la sanción, a lo cual sí se da la revisión por personal designado.

[99] Por el hecho de que las sanciones aplicables responden a una restricción o eliminación del acceso al servicio contratado por el jugador infractor, así como el hecho de que estar sometido a términos y condiciones aceptados como parte del contrato principal suscrito.

[100] Esta conducta se considera sancionable no sólo por lo indicado de que puede dejar en desventaja a jugadores en partidas por equipos, sino porque puede responder al intento del jugador infractor de que no perjudique la ratio de victorias o puntos en clasificatorias o en ranking de jugadores.

[101] En algunos casos, se cuenta con funcione nativas de grabación de fragmento, pero lo habitual es que se graben todas las partidas ocurridas en el juego.

Figura 5. Captura del formulario de denuncia de jugadores por realización de trampas o conductas inapropiadas del videojuego Vanguard.

Las sanciones a aplicar serían las mismas que para el caso principal de escaneo y detección de trampas sin denuncia: desde la restricción en alguna partida, la imposibilidad ganar experiencia que dé acceso a niveles o mejoras o la restricción temporal de juego a suspensión total y completa. Todo ello en base de promedio a cuatro criterios principales.[102]

- **Reiteración**: se escala la sanción si se detectan infracciones previas cometidas por el mismo jugador, en atención a que se incorporarán a un perfil único de jugador;

- **Gravedad**: en función del perjuicio ocasionado se podrá valorar la misma, pero partiendo, en la mayoría de caso, de una pauta de escalabilidad desde un aviso previo sin sanción a una 1º sanción más liviana como advertencia final;

- **Simultaneidad de sanciones**: la posibilidad de sancionar por varias conductas distintas si se comenten al mismo tiempo; y

- **Posibilidad de reclamación** sólo después de la aplicación de la sanción decidida.

2.4.2. Información a los jugadores

Siguiendo la pauta ya indicada de no establecer información específica en la política de privacidad, aun cuando fuera un tratamiento en la que se van a gestionar datos, se divide la información en tres documentos separados y accesibles desde fuera del juego[103]:

[102] No en todos los casos objeto de valoración se pondera de la misma manera. En el caso de Valve con el sistema VAC se estipula un enfoque más duro sin escalada, junto con restricciones de particularidades de dicha plataforma: imposibilidad de venta en el sistema de mercado interno, o participación en el sistema de modificación o «*modding*».

[103] A nivel del 1º acceso al ámbito multijugador del juego, se muestra la indicación reducida de comportamiento adecuado, o aceptación de tres reglas de comportamiento principales, como se mostrará en la 1º captura del apartado 2.8 de propuestas de mejora.

- **Códigos de conducta**: documento que se configura como principal en la materia, pero que no incluye más que pautas generales de comportamiento adecuado;

- **Preguntas frecuentes para denunciantes y denunciados:** documentos más útiles por contener de manera concreta las distintas reglas y supuestos concretos que se puedan dar; y

- **Política de seguridad de cumplimiento**: en casos concretos, como el de Activision, se dispone de una política específica que regula cada tipo posible de infracción y las consecuencias previstas por su 1ª comisión o por reincidencia.

En ninguno caso analizado, al igual que con la prevención de trampas, se dispone de información de 1ª capa que le permitiera al jugador ser informado con anterioridad al tratamiento de sus datos. Al igual que se ha especificado en el tratamiento de prevención de trampas, el único responsable que da información suficientemente concreta como para considerarla como tal, es Riot en el siguiente fragmento relevante:

«D. Comunicación y comportamiento del jugador

Hemos proporcionado herramientas a nuestros jugadores para que nos ayuden a aplicar nuestras políticas (por ejemplo, las que son sobre usos y comportamientos aceptables que publicamos cada cierto tiempo en nuestros sitios web, aplicaciones y juegos) relacionadas con determinados comportamientos en el juego. Por ejemplo, los jugadores pueden denunciarse y enviar información acerca de su actividad y sus acciones en el juego para ayudarnos a determinar si el comportamiento denunciado constituye una infracción de las reglas y los procedimientos aplicables a la conducta de los jugadores, así como posibles repercusiones (como suspensiones de cuenta o restricciones del chat temporales o permanentes). ……..

Usamos herramientas y técnicas tanto manuales (como el permiso para denunciar estas conductas mediante solicitudes de asistencia al jugador) como automatizadas (como el aprendizaje automático, la transcripción y el análisis) para apoyar estos esfuerzos.

Para poder supervisar el cumplimiento de nuestras políticas, desarrollamos plantillas de patrones de comportamiento inadecuado (por ejemplo, abuso, apología del odio, trampas, amenazas, nombres ofensivos o inadecuados), que consideramos indicativos de comportamientos prohibidos. Para ello, nos basamos en un análisis de comportamientos reales en los Servicios de Riot.

Estos patrones de comportamiento inadecuado se clasifican en función de su gravedad con distintas consecuencias (por ejemplo, restricciones de cuenta o de comunicación temporales o permanentes) para los jugadores según la transcendencia de su conducta.

Si otro jugador presenta una queja sobre su comportamiento, nuestras herramientas automatizadas utilizan estos patrones de comportamiento inadecuado y sistema de clasificación para compararlos con su comportamiento a lo largo del tiempo y, si se determina que su comportamiento es inadecuado, para tomar una decisión sobre las consecuencias que este tendrá para usted. Principalmente, esto nos permite aplicar nuestras reglas y políticas, proteger los Servicios de Riot, detectar e impedir actividades no autorizadas y mantener la integridad competitiva de nuestros juegos.

Nuestro procedimiento de quejas puede permitirle recurrir una decisión. En este caso, podemos proporcionarle la información que muestra nuestra justificación y los factores que contribuyeron en la toma de la decisión, junto con algunos consejos sobre cómo evitar que este tipo de comportamiento se repita en el futuro. Si desea recurrirla de todos modos, puede solicitar que uno de nuestros agentes revise su caso. Este tomará una

determinación final manual sobre el resultado correcto en función de las pruebas disponibles.»

2.4.3. Aplicabilidad de la DSA

De manera similar a una primera lectura de la ley de protección del denunciante comentada al inicio del apartado, parecería que cualquier plataforma desde la que juega debería ser considerada como una «*plataforma en línea*» del «Reglamento 022/2065*,* relativo a un mercado único de servicios digitales» («*DSA», por sus siglas en inglés y su denominación en adelante, o «Ley de Servicios Digitales» en su denominación más concreta)*.

En aplicación del tenor literal de la definición del artículo 3.i. de la DSA, ninguna de las plataformas objeto de estudio (*ni en ninguna otra de este tipo*) respondería a este concepto, por el hecho de que «*el servicio de alojamiento de datos, a petición del destinario del servicio, para almacenar y difundir información al público*» es una «*característica o funcionalidad menor o auxiliar*» del servicio principal consistente en permitir el juego multijugador; no pudiendo «*ser utilizado sin el servicio principal por razones objetivas y técnicas*».

No obstante, sí se consideran todos los casos como «*servicios intermediarios»* del tipo de «*alojamiento de datos*» de dicha norma europea, por cuanto no puede negarse que parte del servicio consisten en el almacenamiento de información del destinatario, a su petición. El conjunto de obligaciones de esta figura sería limitado en comparativa con una plataforma en línea, pero obligaría a lo siguiente:

- **Obligación de actuación frente a contenido ilícito (*artículo 9*)**: por órdenes remitidas por autoridad judicial o pública competente, siempre que se circunscriba a lo establecido en el artículo 9. Recuerda a lo dispuesto en la «*Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*»: motivada debidamente, información suficiente de la autoridad solicitante, o concreción de la petición para localizar el contenido ilícito, entre otros;

- **Obligación de actuación frente a usuarios concretos (*artículo 10*)**: en términos similares, junto con la justificación legal o la indicación de las posibles cesiones de la información a otras autoridades implicadas, así como la solicitud de información sobre usuarios concretos relacionados con contenido ilícito;

- **Contacto único (*artículos 11 y 12*):** la obligación de designar una vía única de contacto con las autoridades y otra con los propios usuarios. Similar a lo regulado sobre el DPD en su función de contacto único con la autoridad de control, aunque sin obligación de comunicación a registro público habilitado a tal efecto, y matizando una situación similar al contacto y ejercicio de derechos en protección de datos al interesado de dar una vía de contacto;

- **Representante legal (*artículo 13*):** en condiciones idénticas a la obligación del RGPD al respecto, se estipula la designación de una entidad representante en caso de no estar establecido en el Espacio Económico Europeo, pero se diferencia en la obligación de notificación de la identidad y datos a la autoridad nacional designada como «*Coordinadora de Servicios Digitales*[104]»;

[104] En España se ha designado a la Comisión Nacional de los Mercados y de la Competencia para dicho fin.

- **Transparencia (*artículos 14 y 15*)**: obligación de publicación anual de informes sobre actuaciones de moderación de contenido ilícito realizadas, reclamaciones y órdenes recibidas por las autoridades o actuaciones propio proactivas del responsable. Asimismo, en la línea de las obligaciones de explicabilidad del funcionamiento del algoritmo y toma de decisiones del artículo 22 del RGPD, se estipula una información clara al respecto; y

- **Menores**: el propio artículo 14 habla de la obligación de informar adecuadamente a menores sobre condiciones y restricciones de servicio que les sean de aplicación, aunque con la limitación de referirse sólo a aquellos que estén dirigidos a menores, o que sean usado de manera mayoritaria por ellos. En los casos objeto de estudio, existiría un número importante de menores como jugadores habituales de los mismos, especialmente en el conocido Fornite[105].

Aplicado lo anterior a los responsables objeto de estudio, se constata que sólo Riot, Ubisoft y Epic informan someramente sobre la DSA, de la siguiente manera cada uno:

- **Riot**: en página separada de su web se informa de manera general de las obligaciones enunciadas del artículo 11 al 15, aportando mayor concreción y ejemplos del concepto de «*contenido ilícito*» de lo que determina la propia DSA: bienestar animal, infracciones consumo, infracciones protección de datos, discurso ilícito o dañino o contenido pornográfico. Asimismo, reconoce de manera concreta ser un proveedor de servicios de intermediación del tipo de alojamiento de datos;

- **Ubisoft**: indica un punto de contacto único en los ´términos y condiciones, y dispone de una página informativa y de contacto para petición por parte de autoridades, de conformidad a los requisitos del artículo 9 y 10. Asimismo, en la información de preguntas frecuentes sobre denuncias se informa del punto único de contacto;

- **Epic**: al final del documento de términos del servicio, informa del nombramiento de su filial como representante y del cómputo de los usuarios activos que se consideraría de relevancia para determinar si sería un «*proveedor de muy gran tamaño*» *(«VLOP», por sus siglas en inglés*), sometido a las obligaciones reforzadas que tiene todas las entidades designadas por la Comisión Europea hasta el momento[106]. El resultado no llegaría a los 45 millones establecido como límite, pero da indicación de que EPIC se estaría declarando, no como un servicio intermediario, sino como una «*plataforma en línea*» de las que se ha argumentado al inicio del apartado que no correspondería por el tenor literal.

2.5. Grabación de chats de voz

Es uno de los tratamientos más novedosos que se han implementado en los videojuegos como intento de paliar el uso inadecuado y proliferación de determinados discursos poco éticos o contrarios a ley que se suelen dar de manera habitual y en aumento. Los juegos sobre los que se ha probado los sistemas antitrampas objeto de estudio, no son una excepción a la existencia de estas funcionalidades.

Lo más habitual es que existan dos o más sistemas de comunicación entre jugadores en todos los videojuegos de corte multijugador: un chat general antes de partida o por servidor, y un chat en partida para comunicación con jugadores en la misma partida o la

[105] Fuera de los videojuegos objeto de estudio, se podría mencionar el conocido «Roblox» como un ejemplo de videojuegos enfocado a menores y con una predominancia clara.
[106] Entre otras, se encuentra todas las grandes tecnológicas: Amazon, Meta, Apple, Microsoft, Google con los múltiples servicios masivos que proveen, TikTok o Zalando.

posibilidad de chat en grupo seleccionados de jugadores «*amigos*». Todos ellos, al menos lo que estén en partida y en modalidad de grupo de amigos, tienen la posibilidad de ser por voz.

Este tipo de sistemas que, al igual que el supuesto principal de prevención de trampas y las denuncias de otros jugadores se encontraría sometido al artículo 22, a la evaluación de impacto y a la problemática del interés legítimo; tendrían los siguientes elementos añadidos de posible discordancia en la valoración o juicio de proporcionalidad, idoneidad y necesidad:

- **Falta de información al jugador**: no se da información de 1ª capa al jugador para permitirle conocer el alcance del mismo, qué chats o funcionalidades de comunicación se encuentran sujetas a escaneo, revisión y aplicación de sanción, en su caso.

  Existe una información básica, tal y como se muestras en la captura de este apartado, pero se encuentra en la pestaña u opción de chat de voz, es decir, que el jugador sólo podría entenderse informado previamente (*no en términos exactos del artículo 13 del RGPD*), si entra a modificar parámetros con antelación al inicio del juego. Al igual que en los casos anteriores, la información más concreta sobre qué modera, cómo lo hace y si se aplica como sanción automática; se da en preguntas frecuentes al respecto.

  En el caso de Riot, como parte de la información combinada ya indicada del tratamiento de prevención de trampas y de denuncias, se incorpora una breve referencia, aunque aduciendo que no tienen obligación ninguna de hacerlo y que se reservan el derecho a ello si lo consideran. «*También registramos, almacenamos y nos reservamos el derecho de supervisar (aunque sin obligación alguna) el chat de voz y texto y otros detalles similares sobre las interacciones opcionales durante un período que consideramos adecuado para, entre otras cosas, abordar comportamientos disruptivos, mejorar nuestros servicios, aplicar nuestras reglas y políticas, así como los Términos de servicio, y fomentar una comunidad de juego más positiva para los jugadores».*

  Solamente en el caso analizado del videojuego Warzone (*sistema antitrampa Ricochet de Activision*), se ha mostrado una única vez en el 1º acceso a partida un indicador informativo breve de que el chat de voz en partida será grabado y analizado.

- **Configuración por defecto activada**: el hecho, como se indicará en la captura de ejemplo, de que todas las opciones de limitación o de desactivación del chat de voz se encuentra activadas por defecto, es decir, que empezaría a grabar, analizar y sancionar desde el momento en el que el jugador activara el micrófono y entrara en partida u otra área con chat. El único elemento de control que, en algunos casos se da, es la necesidad técnica de mantener pulsado un botón para poder hablar y activar la funcionalidad;

- **Expectativa razonable del jugador:** todo lo anterior impacta en la expectativa razonable del jugador sobre que se analice lo que diga en partida que pueda ser constitutivo de lenguaje inapropiado o conducta contraria a la ley o términos aplicables, pero no la previsión necesaria de grabación continua y por defecto sin mayor información o activación;

- **Alternativas menos invasivas**: el hecho de que existan sistemas alternativos de comunicación en partida por gestos o frases preconfiguradas seleccionables

para indicar lo necesario en la misma[107], la falta de necesidad de mantener chats generales que son usados de manera inadecuada por los jugadores, la existencia de servicios de uso común compatibles para conectar voz con jugadores amigos en partida y la posible limitación del chat de voz a los jugadores que se acepten como amigos para partidas concretas y limitado a conexión entre ellos;

- **Tratamiento del artículo 22:** unido a lo anterior, la no necesidad de establecer un sistema totalmente automatizado para la realización de este tratamiento más secundario y controlable que el principal de prevención de trampas, tal y como muestra el hecho de que Activision lo implemente de este modo. Asimismo, por especificarlo en sus preguntas frecuente creada a tal efecto[108]:

  «El sistema de moderación del chat de voz de Call of Duty solo envía informes sobre comportamientos tóxicos, clasificados por su tipo de conducta y un nivel de gravedad basado en un modelo evolutivo. Activision determina cómo aplicará las infracciones de moderación del chat de voz.»

- **Posible combinación de datos de otras fuentes o de conjuntos de datos distintos:** unido al hecho de que la legitima expectativa[109] del jugador infractor llegaría a que detectará si emite alguna palabra categorizada por indebida por el algoritmo en una conservación, está el siguiente riesgo de cruce que referencia Activision sin concreción suficiente, en esas mismas preguntas frecuentes del punto anterior:

  «La detección se efectúa en tiempo real. El sistema categoriza y marca el lenguaje ofensivo sobre la base del Código de conducta de Call of Duty cuando lo detecta. Puede que necesitemos revisar grabaciones asociadas a las infracciones del código de conducta que detectemos para poder identificar el contexto antes de determinar qué sanción aplicamos. Por lo tanto, no tomaremos medidas al instante. Nuestros procesos y tiempo de respuesta evolucionarán a medida que desarrollemos el sistema.»

- **Intensidad del tratamiento:** el hecho de que el tratamiento se realice en tiempo real y de manera continua, junto con las limitaciones o restricciones que se implementen para ponderarlo con los derechos y libertades de los jugadores: si el sistema está continuamente monitorizando en partida o en cualquiera área del cliente si se tiene activado el micrófono sin silenciar , o si se realizan un almacenamiento de todas las conservaciones que se monitorizan, entre otros elementos de valoración al respecto; y

- **Control efectivo del jugador:** a diferencia del supuesto principal de no tener opción que reportar o esperar a la expulsión del jugador infractor, en el presente

[107] Los conocidos menús circulares con opciones de acción preconfiguradas para indicar posición del contrario, acciones útiles en partida u órdenes preconfiguradas a otros jugadores del equipo con un único clic o marcación. Asimismo, las opciones de dibujo temporal en juegos de corte de estrategia con formaciones en batalla, como el conocido modo multijugador de la saga Total War.

[108] «*Preguntas frecuentes sobre la moderación del chat de voz de Call of Duty. Una descripción general de la iniciativa beta de Call of Duty para mejorar el chat de voz. La información está sujeta a cambios*.», actualizado a fecha de 11/08/23.

[109] Uno de los supuestos del listado de evaluación para considerar la necesidad de realización de evaluación de impacto, y, que el EDPB en sus «*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*», pone de relieve el impacto negativo sobre la expectativa razonable o legítima del interesado. Penúltimo párrafo, pág. 6.

caso de chat de voz cada jugador puede decidir silenciar de manera individualizada en todo momento a los jugadores que considere oportuno. Asimismo, el elemento adicional de la «*desactivación del chat de voz*», que puede inducir al error de que el tratamiento se base en un consentimiento nunca dado por dicha "*revocación por desactivación*".

Figura 6. Combinación de dos capturas de la información de grabación de chat de voz de Fornite (izquierda) y de los ajustes preconfigurados de chats de grupo de amigos y por equipos de videojuego Vanguard (derecha); sobre los elementos mencionados de la preactivación por defecto y que la información al jugador sólo está dentro de la pestaña sobre este tema.

2.6. Aplicabilidad de la IA Act o RIA

Por el hecho de que todos los sistemas antitrampas objeto de estudio son algorítmicos, así como por la aprobación de texto definitivo del Reglamento europeo de Inteligencia Artificial (*conocido coloquialmente como «IA Act»)* y de su entrada en vigor[110], se considera de relevancia analizar la posible aplicación de dicha norma y sus obligaciones al caso concreto.

En aplicación de la definición del artículo 3.1 del Reglamento de IA, (*referenciado en adelante como «RIA*»), podrían considerarse este tipo de sistemas antitrampas automatizados como un software o sistema de Inteligencia Artificial en sentido estricto de la definición (*muy semejante en el fondo al artículo 22 del RGPD*) dada en este artículo: «*el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de*

[110] Entró en vigor el1 de agosto de 2024, con aplicación efectiva en dos años desde su entrada y escalonada: sistemas de IA prohibidos o inaceptables a los 6 meses, sistemas de alto riesgo, gobernanza, modelos de IA de propósito general y sanciones a los 12 meses, y obligaciones para sistemas de alto riesgo a los 36 meses.

objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa».

Asimismo, por encajar concretamente en los tipos de técnicas que el anexo I del RIA estipula:

- *«Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo»;*

- *«Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico)»; y*

- *«Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización.»*

No obstante, partiendo de la evidencia de ser un sistema de inteligencia artificial, se considera que no podrá justificarse que estuvieran dentro de subgrupo de sistemas de «*IA prohibida*» o de «*riesgo inaceptable*», por las siguientes razones:

- **No serían sistemas prohibidos** por no responder a ninguno de los supuestos concretados como numerus clausus en el artículo 5 del RIA. Los dos únicos supuestos que podría ser objeto de hipotética valoración a este respecto, sería los relativos a la alteración sustancial del comportamiento o que provoquen daños físicos o psicológicos en el usuario, o los que exploten vulnerabilidades de persona o un colectivo sensible en este sentido (*artículo 5, supuestos a.) y b.).*

  En los sistemas actuales y los de objeto de comentario, no podría considerarse que despliegan este tipo de efectos sobre el usuario en sentido estricto. Sí podría justificarse en función a otro tipo de tratamiento que sí se prevalen de la necesidad de generar una respuesta emocional o irreflexiva en el jugador. Por ejemplo, los relativos a la segmentación publicitaria y comportamental que reorganiza la página de compra de la interfaz del juego por todo el perfilado de compras, tipología de géneros jugados, acciones realizadas durante los juegos u otros parámetros relevantes; el diseño de determinados elementos usando patrones oscuros; o los tratamientos de dificultad dinámica[111] o alteración del emparejamiento en partida para intentar maximizar el intento de adquisición de microtransacciones.

- **No sería sistemas de IA de alto riesgo**, por no encontrarse en el listado tasado, igualmente, que propone el artículo 6 del RIA en su triple vertiente: no ser uno de los sistemas o elementos de seguridad de ninguno de los productos de la normativa europea del anexo I, no ser uno de dichos sistemas que implicará por dicha normativa estar sometido a evaluación previa al lanzamiento al mercado por autoridad competente, ni ser uno de los supuestos referenciados en el anexo III[112].

[111] La existencia de sistemas de dificultad dinámica se ha negado de manera específica por muchas editoras de videojuegos de éxito, pero se ha reconocido en comparecencias públicas su uso sobre la competencia directa: Punto 104 del apartado 4, pág. 37 del documento «*Immersive and addictive technologies*» elaborado por el Parlamento Británico tras las comparecencias de especialistas en la materia y representantes de la industria».

[112] Sistemas de identificación biométrica y categorización de personas físicas; infraestructuras esenciales; educación y formación profesional; de gestión, empleo o ámbito laboral; servicios públicos o privados esenciales; de aplicación de la ley o «*law enforcement*»; de migración o asilo;

En conclusión, se considera que quedaría como un sistema de riesgo limitado con la aplicación efectiva de las obligaciones de transparencia establecidas en el artículo 50: *«Los proveedores garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA, excepto en las situaciones en las que esto resulte evidente debido a las circunstancias y al contexto de utilización.«*

Todo lo anterior, sin perjuicio, de la adopción voluntaria de códigos de conducta, de conformidad al artículo 95 de la RIA, en términos similares de revisión y control por autoridades del RGPD.

Al considerarse que no existirían técnica subliminal alguna de las determinadas como actuaciones prohibidas por el RIA, no podría realizarse comentario al respecto. Sí debería ser un elemento valorativo en el ámbito de determinados videojuegos, especialmente de corte móvil y con modelo de negocio gratuito o «*freemium*» con micropagos., en la misma línea de aplicación de los patrones adictivos ya comentados.

A este respecto, la entidad de representación del sector, ya mencionada en el apartado 2.2.6 sobre derecho de acceso, ISFE, avisó de la posible problemática en dos sentidos[113]. Aunque sin mencionar que la vertiente problemática de inducción, ya sancionada por afectar a menores de los micropagos, está presente y sin regulación específica[114]:

- Que cualquier elemento que por jugabilidad se incorpore para provocar una reacción concreta, podría considerarse como un estímulo subliminal prohibido;

- El literal de «*distorsionar materialmente sus comportamientos de manera que les cause o pueda causarles daños psicológicos*» puede dar lugar a interpretaciones muy abiertas y sin poca certidumbre.

2.7. Neurodatos, privacidad mental y seguimiento ocular

Es uno de los grandes temas de futuro cercano, como demuestra el hecho de que las autoridades de protección de datos y de otras materias relacionadas estén publicando documentos en los que se aterrizan los conceptos de neuroderechos, neurodatos, privacidad mental o las distintas categorías de todo esto que se manejan a nivel académico y de investigación. A este respecto, el reciente informe que la propia AEPD y el EDPS han publicado a finales de junio de este mismo año 2024[115].

El ámbito de los videojuegos es un sector en el que esta especialidad va a tener en el futuro una gran incidencia y problemática, tal y como muestra el supuesto concreto que en dicho informe se da sobre el control del juego por la actividad cerebral del jugador. Dicho ejemplo se considera basado en el caso real de conocida creadora de contenido «*Perrykaryal*» que enfoca su contenido en grabarse jugando a títulos conocidos con el uso de sensores de encefalograma y modificaciones a tal efecto.

Aunque esta posible problemática para la protección de datos y privacidad se encuentra referenciada en patentes de sistemas ya comercializados, se considera que lo más

---

o de administración de justicia. A razón del listado original incluido en el RIA en vigor, y sin perjuicio de futuros cambios del listado realizados por la Comisión Europea, en el marco de su competencia atribuida al respecto.

[113] En su documento «*Observations on the proposal for an AI Act*», puntos 10, a, b y c, pág. 3, marzo de 2022.

[114] El mismo ámbito en el que la AEPD pone énfasis en el referido informe de patrones adictivos, con ejemplos concretos sobre técnicas utilizadas en los videojuegos. Por ejemplo, el famoso «*grinding*», recompensas periódicas o «*endowment*».

[115] Informe conjunto AEPD - EDPS «*Neurodatos*», en el marco de los informes y documentos explicativos sobre tecnología emergente del EDPS, llamado «*Tech Dispatch*»

inmediato a nivel de implicación de protección de datos serían los sistemas de realidad virtual con su funcionalidad de seguimiento ocular o «eye tracking, por las siguiente dos razones:

- La percepción en el gran público no se consideraría (*o sería más complicado su extrapolación*), tan invasiva y peligrosa como podría ser cualquier tipo de medición del impulso cerebral o la necesidad de portar sensores de este tipo; y

- Es algo más inmediato que puede permitir a los grandes fabricantes y proveedores (*entre los que se encuentra META con sus Oculus*), conseguir:

    - Perfilado comercial o comportamental mucho más ajustado por la medición de los movimientos involuntarios del ojo que delatarían si algo es del agrado o no de la persona., o porque todo el visor es el propio campo de visión principal del jugador que no podría evitar mirar;

    - Posibilidad de saber si se está diciendo la verdad o no a cualquier cosa que se pregunte, por el análisis del movimiento involuntario de los ojos del jugador;

    - El estado de ánimo del jugador por los mismos movimientos involuntarios oculares, por gestos faciales;

    - Posibilidad de inferir un patrón del sueño, cualquier trastorno ocular o de otra índole[116]; o

    - Reconocimiento de iris u otros elementos únicos del globo ocular para múltiples fines.

2.8. Propuestas de mejora

Dentro del enfoque práctico pretendido en el presente estudio, se expondrán 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 para los responsables objeto de estudio, sin referenciar meras indicaciones de cumplimiento de los elementos faltantes en aquellos supuestos que estuvieran cubiertos parcialmente.

A fin de poder ejemplificar mejor lo que se propone en el presente apartado, se incluirán capturas reales que se considera que muestran contenido aprovechable para mejor el cumplimiento en materia de protección de datos.

2.8.1. Privacidad por diseño y por defecto

En el marco de poder garantizar el cumplimiento del artículo 25 y los elementos nucleares del RGPD desde el diseño del sistema y con las mayores garantías por defecto, se propone las siguientes medidas:

- Por defecto, se encuentren todas las funcionalidades que pudieran afectar a privacidad y protección de datos desactivadas. Por ejemplo, las referidas a la visibilidad de determinada información del perfil por otros jugadores, la activación

[116] Actualmente, hay fabricantes de visores de realidad virtual que implementan sistemas de graduación de vista para aquellos jugadores que lo necesitaran. Esto implicaría la posibilidad del acceso y tratamiento para otros fines, especialmente comerciales, del dato de salud de la graduación exacta del jugador con defecto visual.

de la grabación por chat de voz, la participación automática en chats de otro tipo o recepción de invitaciones de amistad;

- Se parta de las usuales secciones o áreas denominadas de «*privacidad*» que permiten solamente modificar el nivel de publicidad de ciertos elementos del perfil, para crear una específica de esta materia que permita el ejercicio de los derechos de protección de datos, especialmente, en modalidad de autoejercicio dentro de la propia plataforma y revocación de consentimiento u oposición. Asimismo, para contener toda la información de protección de datos para consulta; y

- Todo sea accesible desde la propia plataforma en la que el jugador esté accediendo para jugar, sin aplicare técnicas de patrón oscuro para desincentivar determinadas acciones legítimas.

Figura 7. Combinación de dos ejemplos reales sobre las opciones de configuración que se da en materia de chats y funcionalidades de voz de los videojuegos Vanguard (izquierda) y Call of Duty Warzone (derecha), a fin de indicar que sólo sería necesario que de manera predeterminada se configuraran para este todas las opciones desactivadas.

2.8.2 Información

Para mejorar el cumplimiento del principio de transparencia y el deber de información en lo expuesto previamente en el estudio, se proponen las siguientes medidas:

- Que se informe al jugador en el proceso de instalación sobre que lo posibles cambios que se van a realizar en su dispositivo, que dicha autorización no es un consentimiento y el alcance, consecuencias y qué datos analizados por el sistema antitrampas. Todo ello, aprovechando la existencia del mensaje emergente ya

comentado con el texto: «*¿Desea permitir que esta aplicación realice cambios en su dispositivo?*», y las opciones de sí o no[117];

- Implementar un botón o aviso flotante fácilmente reconocible que permita saber al jugador en todo momento que está siendo objeto de tratamiento[118], al igual que se suele incorporar un aviso visible en muchos dispositivos con funcionalidades de micrófono o dictado por voz activadas;

- Implementar el almacenamiento de los logs del análisis realizado por el sistema antitrampas sin elementos o limitación técnica que impidan su consulta por el jugador, a fin de que puede conocerse en detalle los accesos y elementos analizados en cada momento[119];

- Implementar una 1º capa información real y utilizar los elementos de resalte visual y modo tutorial de opciones que ya se usan para guiar al jugador en funcionalidades que se quieren que sepa utilizar (*se muestra en la 1º captura de este apartado la más adaptable al caso*), para conseguir que la información y funcionalidades clave de privacidad sea vista y entendida por el jugador. Asimismo, incluirlo para las derivadas ya comentadas de grabación de chat de voz y denuncias a jugadores;

- Completar las políticas de privacidad de manera que reúnan la información suficiente sobre el funcionamiento y consecuencias del sistema antitrampas, sin necesidad de que el jugador deba buscarla en las referidas preguntas frecuentes o «*FAQS*». Se considera que dichas preguntas frecuentes pueden seguir siendo el documento de mayor detalle de los mismos y responder a un estilo que favorece el entendimiento, pero que quede reflejadas en la propia política con lo comentado y un enlace directo a las mismas;

- Valorar separar la información específica sobre el tratamiento de perfilado y decisión automatizada sobre prevención de trampas[120], a fin de garantizar que el jugador quede plenamente informado de este tratamiento objeto de estudio más invasivo sin que se confunda con el resto realizados por el responsable de manera general. Asimismo, diferenciado del tratamiento similar ya comentado de la grabación del chat de voz.

[117] Esta opción sólo aparecería en el supuesto de un jugador que acceda desde ordenador, ya que en el resto de supuestos, como ya se ha comentado en el apartado de objeto y alcance, el sistema cerrado de consola no permite acceso al mismo y da las mismas opciones de control.
[118] Se tiene presente el hecho de que el Tribunal Supremo, en su Sentencia 3986/2024 de 25 de junio de 2024 (Caso La Liga), considera que la obligación de incluir aviso de este tipo va más allá del límite exigido por transparencia en el RGPD. En el marco del proceso relativo a la aplicación oficial que incluía funcionalidad de activación de micrófono del interesado para captar la posible vulneración de bares y establecimiento de restauración sin licencia de emisión.
[119] Se considera que por seguridad podría ser cifrados, pero con indicación al jugador de cómo poder descifrarlos y consultarlos. O, exportable en el formato de algún programa de análisis conocido y accesible, como los utilizados en el apartado 2.1, junto con la indicación de cómo
[120] El EDPB, en sus directrices de transparencia, establece que los avisos «*push*» o «*justo a tiempo*» son una forma adecuada para mostrar determinada información concreta y clave al interesado. Último párrafo, pág. 23.

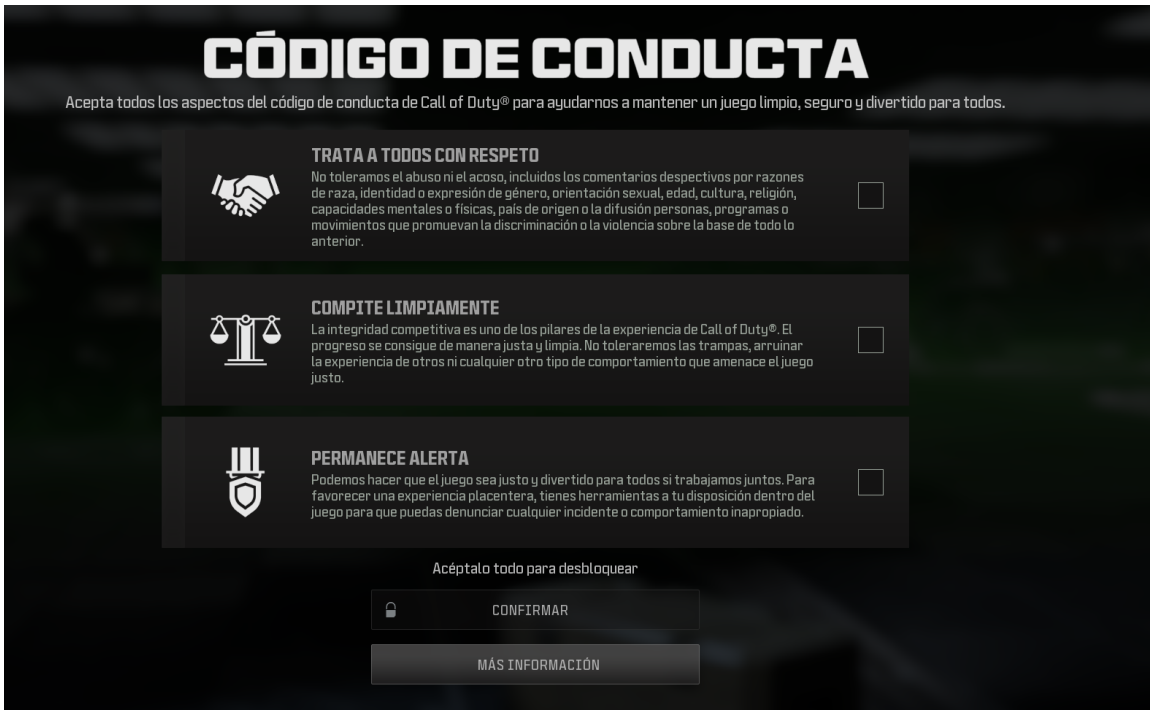


Figura 8. Ejemplo del caso comentado que se considera que podría ser utilizado para informar adecuadamente en materia de 1ª capa con sólo cambiar los textos y adecuarlo los checks a aquellos que en los que fuera necesario consentimiento.

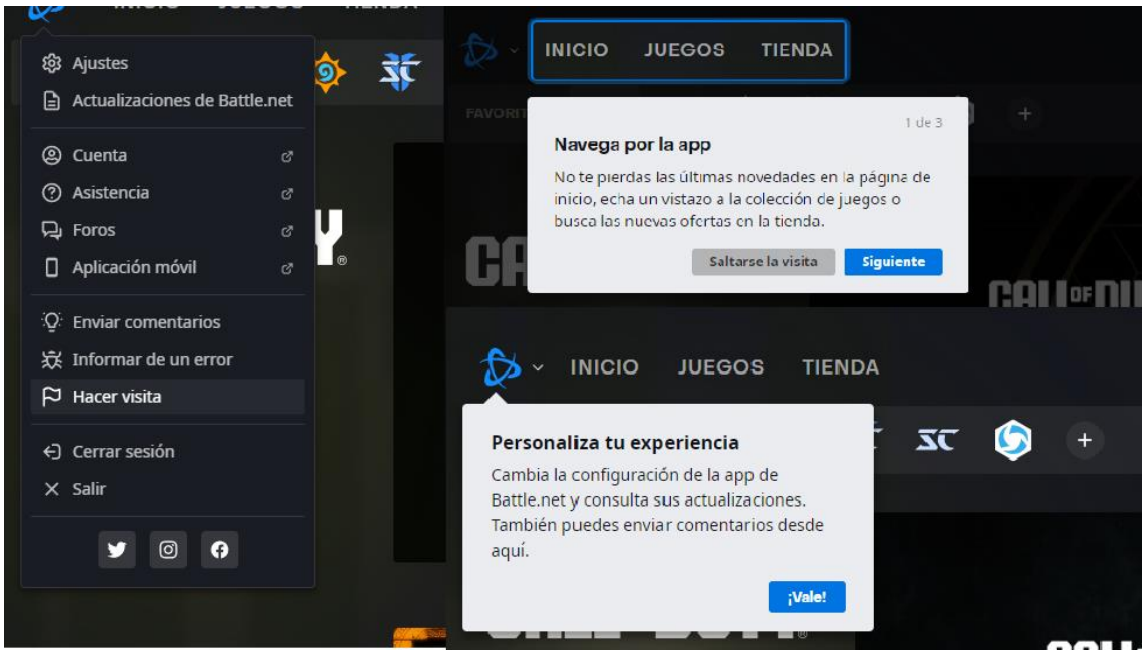


Figura 9. Ejemplo real del «modo de visita» que se implementa como funcionalidad habitual para que el jugador comprenda cómo navegar en su perfil y, que, podría ser fácilmente aprovechado para informar en materia de protección de datos. La implementación mostrada facilitaría la comprensión por añadir el punto de «gamificación» al que un jugador está acostumbrado en cualquier tutorial de juego.

2.8.3. Menores

De conformidad a lo ya comentado del código de conducta del ICO sobre diseños adaptados a diferentes rangos de edad, se proponen las siguientes medidas:

- Permitir que los menores elijan entra una opción escrita o de video/audio para mostrarles la información de protección de datos. Puesto que la industria de los videojuegos está habituada a hacer tutoriales dinámicos en vídeo o interactivos;

- Aportar a los menores materiales escritos o audiovisuales en el momento en el que intenten cambiar la configuración por defecto de privacidad;

- Explicar a los menores qué son los controles parentales que sus padres o tutores podrían aplicar sobre ellos con un estilo de información similar a lo dicho. Asimismo, darles a los padres o tutores información similar;

- Implementar alguna alerta o indicación que permita al menor conocer si está siguiendo objeto de vigilancia paternal o tutoral;

- Implementar una opción, botón o sistema que permita al menor obtener asistencia online ante problemas o incidentes;

- Rediseñar el tono y estilo de escritura de la política de privacidad para que sea entendible por mayores de edad y menores sin crear dobles informaciones. A este respecto, se podría dividir visualmente la política de privacidad en una doble columna: a la izquierda la política de privacidad íntegra, y a la derecha, unas tres o cuatro líneas de resumen del contenido clave de cada apartado;

- Implementar de manera proactiva las obligaciones que el «*Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales*» estipula para los fabricantes de dispositivos: informar de medidas y riesgos sobre con la privacidad y seguridad; informar sobre el tiempo recomendado de uso adecuado a edad; o sobre sistemas de control parental. Asimismo, el elemento de que toda la información se haga con el «*lenguaje accesible, inclusivo y apropiado para todas las edades*» que dicho anteproyecto prevé para los posibles riesgos para el acceso a contenido perjudicial;

- Implementar un sistema de verificación de edad efectivo y no invasivo, siguiendo todo lo que se va concretando a nivel europeo. Lo ya comentado de las pautas de la AEPD, el enfoque de la Cartera Digital Beta, lo propuesto a nivel francés sobre tercero de confianza, o una solución propia que intente evitar el uso de sistemas de reconocimiento facial, biometría o «*estimación facial*[121]»; o

- En línea de todo lo anterior, aprovechar el sistema de cuentas separadas para jugadores menores y mayores de edad, que muchos ya tienen, para adaptar la propuesta de la CNIL de listas blancas y negras para facilitar el control y configuración del padre o tutor sobre las funcionalidades que quiera permitirle al menor en cada momento[122].

2.8.4. Denuncias de otros jugadores

Partiendo del punto de que la implantación de un sistema no totalmente automatizado del artículo 22 en todo el proceso de denuncia, no sería viable desde un punto de vista

[121] Uno de los sistemas que mayor predicamento empiezan a tener a nivel de la industria sobre el ejemplo de «*Yoti: Privacy-Protective Facial Age Estimation*», El ICO, en su «*Regulatory Sandbox Final Report: Yoti A summary of Yoti's participation in the ICO's Regulatory Sandbo*x», de abril de 2022, matiza necesitar más información sobre el tratamiento o no de datos sensibles.
[122] Opinion «La CNIL rend son avis sur les décrets relatifs au contrôle parental», de 31 de julio de 2023.

de la gestión ordinaria de miles de reclamaciones que los jugadores realizan casi en tiempo real, se considera que se debería reforzar el sistema comentados con elementos extraídos de la normativa de denuncias:

- **Información de 1º capa**: se debería incorporar una información básica que permitiera al denunciante conocer el tratamiento de sus datos personales realizado, así como el hecho de que se le comunicará por correo electrónico u otra vía actualización del estado de su denuncia[123];

- **Seudonimizacio**n: obligación del denunciante de utilizar un seudónimo distinto al que tiene como nombre de jugador (*el responsable conocería el nombre 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;

- **Información al denunciado**: de conformidad a lo dispuesto por el artículo 14 del RGPD, se debería informar al propio denunciado del que se tratan sus datos sin ser aportados por el mismo, en un plazo máximo de 30 días y sin indicar la identidad o ningún dato del denunciante[124].

  Se considera que no sería de aplicación la excepción limitante del artículo 14.5.b del RGPD[125] relativa a retrasar la comunicación e información al momento más cercano en el que no supusiera un riesgo y obstrucción de la denuncia. En el presente caso, no existiría la posibilidad de un daño significativo al denunciante por denunciar, ni el denunciado podría poner en peligro un sistema que se encuentra diseñado para aplicar la sanción automáticamente;

- **Procedimiento y plazos***:* establecimiento de un procedimiento pautado con plazos concretos por fases para dotarlo de mayores garantías para ambas partes. Asimismo, que la referencia a dicho procedimiento se incorpore de manera concreta en los referidos códigos de conducta que actúan como documento de consulta principal;

- **Minimización:** advertencia al denunciante de que sólo incorpore a su reclamación los datos concretos de la partida objeto de trampa, minutaje y presunta trampa cometida; pero sin intentar adjuntar ninguna otra prueba en formato de vídeo, información de terceros sobre otras sanciones, partidas o datos del mismo jugador fuera del ámbito denunciado o nombres reales de ninguna parte. Asimismo, configurar el sistema para borrar de manera segura la información indebida que pudiera haber suministrado el jugador denunciante; y

- **Proceso de reclamación:** atendiendo al hecho ya comentado de que todo el procedimiento de denuncia, gestión y asignación de sanciones es completamente automatizado por funcionamiento del servicio, se considera que pudiera mantenerse en los casos menores de necesidad de expulsión en partida para garantizar que el resto de jugadores no sufran perjuicio.

---

[123] En la mayoría de casos se abre un registro actualizable en el que se comunicará al denunciante el estado de la misma.

[124] Pauta establecida en el artículo 31.1 de la Ley de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

[125] «*(…..) en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información*»

Dicho lo anterior, podría establecerse para el resto de infracciones de mayor calado la necesidad de que el sistema comunique y dé un tiempo concreto de reclamación al presunto infractor antes de aplicar la sanción. De tal manera que el sistema quedará establecido sobre una doble reclamación:

- La posibilidad de presentación de pruebas en un tiempo concreto y limitado para evitar la aplicación de sanciones que excedan la expulsión de la partida concreta. Por ejemplo, expulsión por periodo más amplio, limitación de funcionalidades concretas, prohibición de juegos online multijugador, imposibilidad de compra o expulsión; o

- La ya existente posibilidad de reclamación tras la sanción con revisión humana.

Basadas en la DSA, sobre la base de las obligaciones del proveedor considerado como plataforma en línea[126], se proponen las siguientes medidas a aplicarse de manera proactiva:

- Sistema interno de gestión de reclamaciones que permita a los usuarios poder reclamar decisiones de bloqueo del acceso o visibilidad, suspensión del servicio o restricción de cualquier tipo;

- Configuración técnica para que la creada figura del alertador fiable tenga prioridad en las notificaciones que comunique, como consecuencia de la mayor confiabilidad que le otorga dicha posición validada por autoridad nacional designada [127].

- Suspensión del servicio a los usuarios que de manera frecuente aporten contenido que se considere ilícito; y

- Obligación de diseño de las interfaces de manera clara y que no incluyan ningún tipo de patrón oscuro.

2.8.5. Certificaciones y marcas de privacidad

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 que salen al mercado con información clave de su contenido, se plantea la creación de una marca 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, así como permitir una homogeneización a nivel de todo el Espacio Económico;

- Sea concedida tras un proceso de valoración o certificación de cumplimiento, con un límite de vigencia y auditorías periódicas de renovación y control al estilo de cualquier norma técnica;

[126] Las principales obligaciones se encontrarían reguladas en los artículos 20 a 28 de dicho Reglamento.

[127] En determinados videojuegos, como, por ejemplo, Counter Strike Global Offensive, existía una figura sin regulación que pudiera tener un paralelismo con la presente: el revisor de fragmentos o «*clips*» de determinados minutos de partida denunciados por otros jugadores, que actuaría como 1º filtro de garantía por acreditarse un número mínimo de horas jugadas que prueba un conocimiento profundo del mismo.

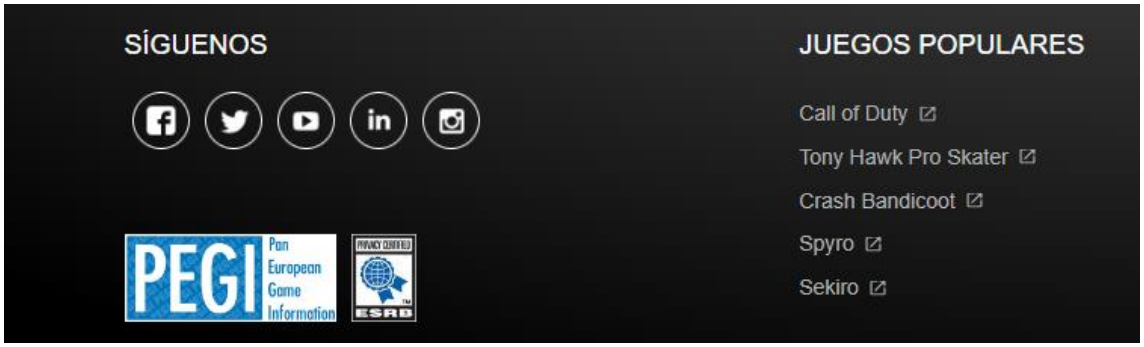
- Sea parte de las obligaciones del responsable recogidas en un código de conducta creado a tal efecto; y

- Sea complementado con una indicación específica dentro del diseño de la propia etiqueta de la región o conjunto de países en la que se considera válida, a fin de informar adecuadamente a jugadores y padres de que en su país es adecuado. Por ejemplo: UE junto a Noruega, Islandia o Liechtenstein; Estados Unidos o China, entre otros países.

Este punto se considera de relevancia por el hecho de que una parte de los grandes actores informan de la tenencia de certificados válidos a nivel de Estados Unidos en sus páginas web principales que se traducen al idioma correspondiente según detecte la IP del usuario. Este tipo de etiquetado sólo indicaría que, a nivel de Estados Unidos, la entidad de etiquetado de videojuegos, ESRB, constata un hecho sin consecuencia legal a efectos del RGPD. Además de la visibilidad de dicha etiqueta, el jugador o usuario puede caer en el error de ser aplicable a nivel de la Unión Europea, por los dos elementos adicionales:

- El hecho de que en información de contacto y asistente se traduzca e incorpore como parte de la política de privacidad: «*Puede contactar asimismo con la Certificación de Privacidad del ESRB si tiene alguna pregunta o reclamación que no se haya resuelto a su satisfacción. Consulte la sección del Programa de Certificación de Privacidad del ESRB al principio de esta Política de Privacidad para más detalles*.»; y

- El hecho de incorporarla, tal y como se muestra en la captura, al lado del logotipo de la entidad europea de etiquetado de videojuegos, PEGI, con la que no tiene relación. Solamente un jugador o persona con conocimiento de genera de la industria puede llegar a disociar adecuadamente ambas entidades.



2.8.6. Decisiones totalmente automatizadas y perfilado

De conformidad a las recomendaciones dadas por el EDPB para sistemas algorítmicos, en sus directrices sobre decisiones automatizadas ya citadas[128], cabría proponer las siguientes:

- Controles periódicos de aseguramiento de la calidad de sus sistemas para garantizar que las personas reciben un trato justo y no discriminatorio;

- Auditorías algorítmicas para detectar errores o resultado que impliquen un perjuicio injustificado;

[128] «*Anexo 1 - Recomendaciones de buenas prácticas*», págs. 36 y 37.

- Implementar garantías contractuales con los proveedores del sistema que garanticen que la auditoría y la comprobación se han llevado a cabo, o que el algoritmo cumple las normas acordadas; y

- Mejoras en la posibilidad de impugnar la decisión y el mecanismo de intervención humana que se da a posterior de la aplicación de la sanción.

Aprovechando que el ICO, en su documento «*Explaining decisions made with AI*», se proponen seis elementos concretos de los que debería informarse al interesado para puede entender realmente lo que hace y cómo le afecta el algoritmo o sistema de IA que se le aplica. Podrían incorporarse al documento de preguntas frecuentes usado como documento informativo más completo sobre sistemas antitrampas:

- Incluir la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado y medio de contacto;

- Referenciar las características, capacidades limitaciones del funcionamiento del sistema y finalidad, expresado de manera no técnica y clara;

- Incluir información sobre el nivel de precisión, solidez del sistema y las circunstancias conocidas o previsibles que podrían afectar a dicho nivel de precisión y solidez prevista;

- Referenciar cada circunstancia conocida o previsible, asociada a la utilización del sistema de IA conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales;

- Aportar información explicativa a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista;

- Referenciar la vida útil prevista del sistema de IA, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento del sistema. Es decir, aplicación del principio de limitación del plazo de conservación y medidas de seguridad del artículo 32 del RGPD: y

- Configurar el sistema antitrampas para que esa 1ª fase preventiva más invasiva de escaneo del dispositivo del jugador, sea opcional y bajo un derecho de oposición real: previo y ejercitable.

3. Consideraciones finales y conclusiones

Como se ha intentado exponer a lo largo de estudio, la prevención de trampas realizadas sobre los jugadores, especialmente el ámbito multijugador, es uno de los tratamientos más comunes, invasivos y progresivos de cuantos se desarrollan en la industria de los videojuegos.

La situación actual de avance tecnológico continuado del software y elementos de otra índole que permite realizarlas lleva a la industria a una carrera que no sólo incluye una limitación y control de los jugadores cada vez más acuciantes, sino a intentar establecer técnicas de escaneo y control, como la más invasiva que se destaca en este estudio: escaneo en tiempo real con acceso a nivel de administrador del dispositivo del jugador y sus archivos, con el objetivo de detectar preventivamente cualquier posible trampa antes de su comisión. Todo ello de la manera expuesta en el estudio: realizado de

manera completamente automatizada, con efectos jurídico al impedir el acceso a servicio contratado y sin intervención humana por la asignación automática de sanción.

Como elemento adicional de problemática, se ha expuesto la confusión entre el derecho de propiedad intelectual y la protección de datos, de manera que han supuestos dos importantes limitaciones en los resultados y alcance del estudio:

- La imposibilidad técnica de auditar de manera externa los datos personales concretos a los que se tenía acceso en cada caso analizado, en base al bloqueo de cualquier sistema de análisis forense avanzado para proteger su código fuente y propiedad intelectual; y

- La problemática a nivel del ejercicio de los derechos de acceso presentados, aduciendo, sin concreción jurídica, la excepción del 18.5 del RGPD para no dar satisfacción a dicho derecho a ningún nivel. O ignorando completamente la petición y reconduciéndola al sistema automatizado que arroja información sobre los datos recopilados y observados, pero nunca sobre los inferidos y la especialidad solicitada.

Asimismo, se ha intentado aportar concreción suficiente del resto de elementos y funcionalidades que se suman en el ecosistema completo de prevención de trampas y conductas inapropiadas: grabación de chat de voz para detectar conductas verbales contrarios al código de conducta, y la posibilidad de denuncia de resto de jugadores por trampas de las que se sean conocedores en partida.

Como conclusiones principales del estudio, se consideran las siguientes:

- El tratamiento objeto de análisis no se considera, per se, imposible de realizar en base al interés legítimo, pero se considera que se debería aportar las limitaciones y garantías concretas que se referencia en el estudio, y, principalmente, en el apartado de propuesta de mejora. Especialmente, en el hecho de establecer un verdadero derecho de oposición y opcionalidad en la 1º fase de escaneo preventivo del dispositivo, o la problemática de las excepciones habilitantes del artículo 22 para ello;

- Todo lo dispuesto se aplica de manera efectiva a los menores de edad, por cuanto no se dispone de sistemas adecuados de verificación, y se considera un tratamiento troncal aplicado a todo jugador para intentar minimizar el uso de posibles trampas;

- La legitima expectativa del jugador se alinea con la existencia de este tipo de sistemas usados desde hace años, pero nunca al nivel que muchos de ellos realizan sin información adecuada al alcance. Asimismo, la confusión terminológica con los sistemas de DRM creados para garantizar los derechos de propiedad intelectual del juego, que puede implicar una falsa validación para el jugador que debe ser matizada; y

- El hecho ya comentado de posibles alternativas menos invasivas, sea a nivel del propio sistema por limitarse a nivel del servidor; o por el resto de fases que actúan al mismo fin sin el componente de escaneo completo de la 1ª fase.

Se considera que este estudio de análisis jurídico general, junto con la aplicación de la DSA, la entrada en vigor del Reglamento Europeo de IA o la futura normativa de protección de menores y verificación; puede otorgar a los responsables y resto de figuras involucradas, la oportunidad de reevaluar el tratamiento, aplicar garantías, medidas propuestas o adecuar lo máximo posible a efectos de protección de datos y de los jugadores en entorno netamente digital.

Finalmente, se considera que pudiera ser de interés a efectos de las distintas autoridades de protección de datos de los estados miembros para la realización informes, publicaciones, directrices o documentación de ayuda, por cuanto demuestran actualmente un interés más cercano en determinadas cuestiones relativas a la industria de los videojuegos. Por ejemplo, el reciente informe de la propia AEPD sobre patrones adictivos con ejemplos concretos de la materia, la publicación conjunta con el EDPS sobre neuroderechos ya mencionada, o las que el ICO emitió para desarrolladores (*cuando ostentaba el rango de autoridad de estado miembro*): «*Top tips for games designers».*

4. Bibliografía

1) Copia digital de las capturas, logs de análisis técnico obtenidos y copia de información suministrada en el ejercicio de derechos de acceso

1. Enlace al repositorio de documentación en nube europea: https://drive.filen.io/f/0382f181-55fb-4e8d-a560-fd55e13944a6#w2iWxM664rWW1bfxmYJyh80kwuVRqGzU

2) Políticas de privacidad, códigos de conducta, preguntas frecuentes y documentación de los sistemas y responsables objeto de estudio

Activision – sistema antitrampas Ricochet sobre el videojuego Call of Duty:Warzone

1. Política de privacidad. Actualizada el 20 de diciembre de 2022. https://www.activision.com/es/legal/privacy-policy
2. Preguntas frecuentes de Ricochet. Actualizadas el 11 de abril de 2024. https://support.activision.com/es/articles/ricochet-overview
3. Preguntas frecuentes denuncias en Warzone. Actualizada a 14 de noviembre de 2022. https://support.activision.com/es/warzone-2/articles/reporting-a-player-in-warzone-2
4. Código de conducta en forma de política de seguridad. Actualizado el 24 de julio de 2024.
5. «*Informe del progreso de RICOCHET Anti-Cheat*». Publicado el 4 de abril de 2023. https://www.callofduty.com/es/blog/2023/04/call-of-duty-modern-warfare-II-and-warzone-2-0-ricochet-anti-cheat-season-3-update
6. Preguntas frecuentes grabación por voz de Activision https://support.activision.com/es/articles/call-of-duty-voice-chat-moderation

BattlEye – sistema antitrampas del mismo nombre sobre el videojuego de Ubisoft: Xdefiant.

1. Política de privacidad de BattlEye. Sin fecha: https://www.battleye.com/privacy-policy/
2. Política de privacidad de Ubisoft. Actualizada en mayo de 2022: https://legal.ubi.com/privacypolicy/es-ES
3. Información sobre denuncia a otros jugadores Ubisoft. Sin fecha: https://www.ubisoft.com/es-es/help/xdefiant/player-safety/article/reporting-a-player-in-xdefiant/000104608
4. Código de conducta de Ubisoft. Sin fecha: https://www.ubisoft.com/es-es/help/player-safety/article/code-of-conduct-the-way-we-play/000095037
5. Información de colaboración con autoridades y punto de contacto sobre DSA de Ubisoft. Sin fecha. Consultado el 5 de agosto de 2024: https://legal.ubi.com/LegalInfoUbisoftEMEA/es-ES

Valve – sistema VAC sobre el videojuego Team Fortress 2

1. Preguntas frecuentes del sistema VAC. Sin fecha. - https://help.steampowered.com/es/faqs/view/571A-97DA-70E9-FF74
2. Política de privacidad de Valve (plataforma Steam). Actualizada a 14 de febrero de 2024 – https://store.steampowered.com/privacy_agreement/spanish/
3. Código de conducta. Sin fecha: https://store.steampowered.com/online_conduct?snr=100601___

4. Denuncia a otros jugadores. Sin fecha: https://help.steampowered.com/es/faqs/view/4DE7-17AA-0E8B-C1AD

Riot Games – sistema antitrampas Vanguard sobre el videojuego Valorant

1. Política de privacidad. Actualizada a 15 de septiembre de 2023: https://www.riotgames.com/es/privacy-notice-ES
2. Preguntas frecuentes sobre penalizaciones y suspensiones. Actualizado a 13 de abril de 2023: https://support-valorant.riotgames.com/hc/es-419/articles/4402501234451-Preguntas-frecuentes-penalizaciones-y-suspensiones
3. Denuncia a otros jugadores. Actualizado a 4 de junio de 2024: https://support-leagueoflegends.riotgames.com/hc/es-419/articles/201752884-Preguntas-frecuentes-y-gu%C3%ADa-para-reportar-a-un-jugador
4. Información sobre contenido ilícito y aplicación de la DSA de Riot: https://support-leagueoflegends.riotgames.com/hc/es/articles/25972785684627-Contenido-ilegal-informes-y-apelaciones-solo-UE
5. Información de restricciones técnicas del sistema Vanguard. Actualizado a 31 de octubre de 2023: https://support-valorant.riotgames.com/hc/en-us/articles/22291331362067-Vanguard-Restrictions
6. Documento informativo general de sistema Vanguard en su lanzamiento. Publicado en 2020: https://www.leagueoflegends.com/en-us/news/dev/dev-null-anti-cheat-kernel-driver/

Epic Games – sistema antitrampas Easy-anticheat sobre el videojuego Fornite

1. Política de privacidad. Actualizada a 24 de junio de 2024: https://www.epicgames.com/site/es-ES/privacypolicy
2. Código de conducta. Actualizado a 15 de febrero de 2024: https://www.epicgames.com/site/es-ES/community-rules?lang=es-ES
3. Denuncia otros jugadores. Sin fecha: https://www.epicgames.com/help/es-ES/c-Category_Fortnite/c-Fortnite_PlayerBehavior/como-denunciar-el-mal-comportamiento-de-un-jugador-en-fortnite-a000086135

3) Agencia Española de Protección de Datos (AEPD)

1. «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
2. R/00532/2020 - https://www.aepd.es/documento/td-00121-2020.pdf
3. PS/00070/2019 - https://www.aepd.es/documento/ps-00070-2019.pdf
4. Documento «*Patrones adictivos en el tratamiento de datos personales Implicaciones para la protección de datos», julio de 2024*». https://www.aepd.es/guias/patrones-adictivos-en-tratamiento-de-datos-personales.pdf
5. Informe conjunto AEPD - EDPS «Neurodatos», de 27 de junio de 2024. https://www.aepd.es/guias/neurodatos-aepd-edps.pdf

4) Comité Europeo de Protección de datos (EDPB)

1. «Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE», de 9 de abril de 2014: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.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 la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017, Revisadas por última vez y adoptadas el 4 de octubre de 2017. https://www.aepd.es/documento/wp248rev01-es.pdf
4. «Directrices sobre transparencia en virtud del Reglamento (UE) 2016/679», de 11 de abril de 2018 https://apdcat.gencat.cat/web/.content/03documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf
5. «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
6. «Endorsement 1/2018», de 25 de mayo de 2018. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf
7. «Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679», de 25 de mayo de 2018. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf
8. «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
9. «Directrices 4/2019 relativas al artículo 25 - Protección de datos desde el diseño y por defecto», de 20 de octubre de 2020. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf
10. «Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19», de 21 de abril de 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf
11. «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
12. «Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, de 7 de julio de 2021. https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf
13. Análisis encargado por el EDPS sobre la normativa de acceso de autoridades de Chin, Rusia e India - Government access to data in third countries Final Report EDPS/2019/02-13»- Publicado en noviembre de 2021: https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf
14. «Directrices 03/2022 sobre patrones de diseño engañosos en plataformas de medios sociales plataformas de medios sociales: cómo reconocerlos y evitarlos», de 14 de febrero de 2023. https://edpb.europa.eu/system/files/2023-02/edpb_03-

2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
15. «Dictamen 5/2023 sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa al carácter adecuado de la protección de los datos personales en el marco de la protección de datos entre la UE y los EE. UU», de 28 de febrero de 2023. https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf
16. «Directrices 01/2022 sobre los derechos de los interesados - Derecho de acceso», de 17 de abril de 2023. https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf
17. Análisis encargado por el EDPS sobre la normativa de acceso de autoridades de Turquía, Brasil y México: «*Government access to data in third countries II Final Report Specific Contract No. 2022-0716 Implementing the Framework Contract EDPS/2019/02*». Publicado en abril de 2023 - https://www.edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf

5) Autoridad de protección de datos británica (ICO)

1. «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
2. «Regulatory Sandbox Final Report: Yoti A summary of Yoti's participation in the ICO's Regulatory Sandbox», de 22 de mayo de 2022. https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf
3. «Top tips for games designers – how to comply with the Children's code», de febrero de 2023: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/top-tips-for-games-designers-how-to-comply-with-the-children-s-code/
4. 2. «Explaining decisions made with AI». https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/

6) Autoridad de protección de datos francesa (CNIL)

1. «Guía para desarrolladores», de junio de 2020. https://www.cnil.fr/en/gdpr-developers-guide
2. «La CNIL rend son avis sur les décrets relatifs au contrôle parental», de 31 de julio de 2023. https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-decrets-relatifs-au-controle-parental#:~:text=La%20CNIL%20a%20rendu%20un,mani%C3%A8re%20%C3%A0%20prot%C3%A9ger%20leurs%20donn%C3%A9es.

7) Normativa

1. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
2. 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.
3. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

4. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
5. Reglamento (UE) 2022/2065 de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Ley de Servicios Digitales).
6. Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos, de julio de 2024. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52024DC0357
7. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE)

8) Tribunal de Justicia de la Unión Europea (TJUE) y Tribunal Supremo (TS)

1. Resolución del Tribunal de Justicia de la Unión Europea «C-210/16 Wirtschaftsakademie Schleswig-Holstein», de 5 de junio de 2018. http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=10661833
2. Resolución del Tribunal de Justicia de la Unión Europea «C-25/17 Jehovan todistajat», de 10 de julio de 2018. 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», de 29 de julio de 2019. 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 Supremo sobre la obligación excesiva de imponer un aviso de activación del micrófono en cada momento de activación por la aplicación de La Liga. STS 3986/2024 - ECLI:ES:TS:2024:3986, de 25 de julio de 2024: https://media.licdn.com/dms/document/media/D4D1FAQH7gBfivFHIYQ/feedshare-document-pdf-analyzed/0/1722068101361?e=1723075200&v=beta&t=502WeLQGjVX4cQ1Qb6DUS_qMoFplGWdcZ_Hp1-ULOlY
5. Jean Richard De La Tour, Agodado General, 12 de septiembre de 2024. Asunto C-203/22 - Petición de decisión prejudicial planteada por el Verwaltungsgericht Wien (Tribunal Regional de lo Contencioso-Administrativo de Viena, Austria. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62022CC0203&qid=1726212798071
6. Resolución del Tribunal de Justicia de la Unión Europea sobre asuntos acumulados «C-17/22 y C-18/22», de 12 de septiembre de 2024: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62022CJ0017

9) Otros

1. Joel Noguera, Security Consultant at Immunity Inc. Fuente: Unveiling the underground world of ANTI-CHEATS. REcon MONTREAL 2019. https://www.immunityinc.com/downloads/Recon2019_Unveiling_the_Underground_World_of_Anti-Cheats.pdf
2. «House of Commons Digital, Culture, Media and Sport Committee (Parlamento británico) - Immersive and addictive technologies Fifteenth Report of Session 2017–19 Report, together with formal minutes relating to the report», de 9

de septiembre de 2019.
https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf
3. Documento explicativo para clientes de la empresa comercializados del sistema antitrampas Denuvo, indicado que Windows recomienda instalación a nivel de núcleo o Kernel. 2021. https://irdeto.com/hubfs/resources/e-books/denuvo-anti-cheat-windows-kernel-mode.pdf
4. «Robust Vision-Based Cheat Detection in Competitive Gaming», NVIDA y Universidad de California, Aditya Jonnalagadda,,Iuri Frosio, Seth Schneider, Nvidia, Morgan Mcguire, y Joohwan Kim, 18 de marzo de 2021. https://arxiv.org/pdf/2103.10031
5. «Joint ISFE-EGDF Reply to the Public Consultation on the EDPB's Guidelines 01/22 on Data Subject Rights – Right of Access». Marzo de 2022 - https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Joint%20ISFE%20EGDF%20Reply%20to%20the%20EDPB%20consultation%20on%20the%20rights%20of%20access%20FINAL.pdf
6. ISFE «Observations on the proposal for an AI Act», abril de 2022 - https://videogameseurope.eu/wp-content/uploads/2022/09/ISFE-position-paper-AI-Act-2022-April.pdf
7. Recomendación de la utilización del concept en castellano de antirampas, por parte de la Fundación del Español Urgente (Fundeu), 13 de julio de 2022. https://www.fundeu.es/recomendacion/sistema-antitrampas-mejor-que-anticheat/
8. Federal Trade Commission: sanción a Epic por vulneración de la normativa de menores y determinados elementos de privacidad. Diciembre de 2022: https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations
9. «Cheat detection & prevention methods in video games». Universidad de Oulu, Information Processing Science Bachelor Thesis, Heikki Haapaniemi, 2024 - https://oulurepo.oulu.fi/bitstream/handle/10024/48840/nbnfioulu-202404172809.pdf?sequence=1&isAllowed=y
10. US20170352183 – FACE AND EYE TRACKING USING FACIAL SENSORS WITHIN A HEAD-MOUNTED. 2017 - https://patentscope.wipo.int/search/es/detail.jsf?docId=US206644185&_cid=P22-KZ353F-72074-1