Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

RESEARCH ARTICLES
RECPC 27-08 (2025)

Cuando los Videojuegos Dejan de Ser Divertidos. Resultados de Estudio Observacional del Ciberacoso Sexual de menores en Fornite

Facundo Gallo-Serpillo*
Universidad Internacional de La Rioja, Spain.

Leticia Armendáriz
Universidad Internacional de La Rioja, Spain.

Gallo-Serpillo, Facundo and Armendáriz, Leticia. Cuando los Videojuegos Dejan de Ser Divertidos. Resultados de Estudio Observacional del Ciberacoso Sexual de menores en Fornite. *Revista Electró- nica de Ciencia Penal y Criminología*. 2025, núm. 27-08, pp. 1-23.

Resumen: El abordaje de menores en videojuegos con fines sexuales, también conocido como child grooming, representa un problema creciente, facilitado por la naturaleza interactiva, anónima y masiva de este tipo de plataformas de entretenimiento, así como también por la ausencia de supervisión parental y la normalización de discursos violentos. En este contexto, se propone el uso de la etnografía virtual encubierta como metodología clave para la observación directa de dinámicas de ciberacoso en contextos reales, permitiendo identificar patrones de conducta y vulnerabilidades del sistema sin interferir en el entorno digital; esta técnica ofrece datos empíricos relevantes que difícilmente podrían obtenerse mediante encuestas o estudios declarativos. Los resultados evidencian fallos en la prevención, en la notificación efectiva y en la capacidad de reacción de los entornos virtuales como Fortnite, lo que refuerza la necesidad de implementar medidas de protección basadas en restricción por hardware y protocolos de denuncia más ágiles y resolutivos.

Palabras Clave: Grooming Digital; Ciberacoso Sexual Infantil; Menores; Fortnite; Etnografía Virtual; Videojuegos

Abstract: The issue of minors in video games engaging in sexual activities, also termed child grooming, has emerged as a prominent concern. This phenomenon is enabled by the interactive, anonymous and extensive nature of these platforms, as well as by the lack of parental oversight and the prevalent dissemination of violent rhetoric. In this context, the utilisation of covert virtual ethnography is proposed as a pivotal methodology for the direct observation of cyberbullying dynamics in real contexts, thereby facilitating the identification of behavioural patterns and system vulnerabilities without interfering in the digital environment. This technique provides relevant empirical data that would be difficult to obtain through surveys or declarative studies. The results indicate deficiencies in the prevention, effective reporting and responsiveness of virtual environments such as *Fortnite*. This finding serves to reinforce the necessity of implementing protection measures based on hardware-based restriction and more agile and responsive reporting protocols

Keywords: Digital Grooming; Solicitation Of Children; Minors; Fortnite; Virtual Ethnography; Video Games.

Fecha de Recepción: 21 de julio de 2025
Fecha de Publicación en RECPC: 16 de octubre de 2025
Contacto: facundodavid.gallo@unir.net

I. **Introducción**

La Unión Europea (UE) ha declarado la presente década como el "Decenio digital", por la relevancia que ha adquirido la transformación digital en todos los aspectos de nuestra vida. El mundo digital ha tenido efectos positivos en ámbitos tan diversos como la protección de los derechos sociales y políticos de las personas, las relaciones de los ciudadanos con la Administración, la educación, las comunicaciones o el ocio. No obstante, también ha acarreado nuevos problemas y riesgos para la sociedad relacionados con la vulneración de los derechos fundamentales, especialmente los relacionados con la privacidad, la intimidad o la protección de datos; los ataques a los sistemas democráticos; los derechos del consumidor; los ataques cibernéticos a infraestructuras críticas; o el mal uso de la inteligencia artificial (IA)[1]. En este sentido, uno de los principales y más importantes problemas que ha generado el mundo digital es la violencia gestada en los entornos digitales. A través de las tecnologías de la información y comunicación (TIC's) se llevan a cabo diversas modalidades de violencia que afectan de manera particular a colectivos y personas vulnerables. Un tipo de violencia que causa gran alarma social es la de connotación sexual, especialmente si se ejerce contra los niños. De acuerdo con la Observación General núm. 13 del Comité de los Derechos del Niño (2011)[2], los principales riesgos derivados del uso de la red y las TIC's para los menores de edad son los abusos sexuales; la producción de imágenes y grabaciones de dichos abusos; tomar, retocar, distribuir, exhibir, poseer o publicar imágenes indecentes de menores; exponerlos a contenidos agresivos, violentos, pornografía o engañosos, que puedan perjudicarles; o ser acosados, hostigados o intimidados. La violencia de tipo sexual contra menores de edad se ejerce en los diversos entornos digitales a los que estos acceden, incluidos los videojuegos en línea. Estos proporcionan funcionalidades para que los jugadores puedan interactuar de manera anónima, facilitando conductas de tipo sexual contra menores de edad. A nivel internacional y europeo, diversos instrumentos jurídicos y de *soft law* han comenzado a establecer directrices para garantizar entornos digitales seguros para los menores, incluidos los videojuegos en línea, en particular, la observaciones generales Nº 16 (2013)[3] y

[1] Comisión Europea. (2025, octubre 10). *Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065, DOUE Comunicación C/2025/5519*.

[2] Del Niño, C. D. L. D. (2011). Observación general No. 13. Derecho del niño a no ser objeto de ninguna forma de violencia. *Ginebra, Suiza: Comité de Defensa del Niño*. https://www.acnur.org/fileadmin/Documentos/BDL/2012/8603.pdf

[3] del Niño, C. d. l. D. (2013). Observación general No 16 (2013) Sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño. *Recuperado de: https://www.right-to-education.org/sites/right-toeducation.org/files/resourceattachments/CRC_Observaci%C3%B3n_general_16_ES_2013.pdf*.

Nº 25 (2021)[4] del Comité de Derechos del Niño en interpretación de la Convención de las Naciones Unidas sobre los Derechos del Niño (1989), la Comunicación de la Comisión Europea "Brújula Digital 2030: el enfoque de Europa para el Decenio Digital", y la Comunicación "Una década digital para los niños y jóvenes: la nueva estrategia europea para una internet mejor para los niños (BIK+). En este contexto, el presente trabajo que forma parte del proyecto CISEMEVI ofrece los resultados de un estudio empírico observacional sobre las medidas de reacción y protección de los menores frente a indicios de ciberacoso sexual infantil en *Fortnite*, uno de los videojuegos más populares entre los usuarios más jóvenes. El estudio utiliza la metodología de etnografía virtual encubierta con el objetivo de recopilar evidencias empíricas que permitan identificar las brechas de seguridad y mejorar las herramientas existentes o bien desarrollar otras nuevas para garantizar entornos digitales seguros para los menores.

1. ***Delimitación del Ciberacoso Sexual Infantil (Grooming Digital)***

Aunque ampliamente reconocida como una forma de abuso y explotación sexual infantil, la(s) práctica(s) de atraer o captar a niños con fines sexuales no tiene una denominación y definición unívoca, siendo objeto de ambigüedad terminológica y conceptual tanto en el plano académico como en el normativo. La literatura y los medios emplean expresiones como ciberacoso (sexual-infantil), *grooming* (y sus variantes child grooming, online grooming, sexual grooming) *embaucamiento, proposiciones, instigación o captación online, engaño pederasta o abuso sexual digital*, entre otras, en ocasiones de forma indistinta o imprecisa. Esta diversidad terminológica refleja, por un lado, la evolución del fenómeno a medida que cambian los canales donde se produce, o se identifican las tácticas o conductas que lo integran y desarrollan; y por otro, las distintas aproximaciones como objeto de estudio desde disciplinas como el derecho penal e internacional, la psicología forense, la criminología, la victimología o la pedagogía social. A consecuencia de ello, se observa una disociación entre el uso fenomenológico del término y su definición jurídico-penal (el delito). No todo lo que se percibe como *grooming* ni todas las fases del proceso de *grooming* constituye, jurídicamente, un delito de proposición o embaucamiento sexual a menores. Por ello, antes de explicar los resultados estudio empírico realizado en el videojuego *Fortnite*, abordamos su delimitación como fenómeno y como delito en Derecho internacional, explicando a su vez la elección del término ciberacoso sexual infantil y/o *grooming digital* para referirnos al objeto de estudio. Desde el punto de vista fenomenológico, la atracción y manipulación emocional de menores con fines sexuales es una práctica que antecede a su reconocimiento jurídico internacional. Incorporado como delito

[4] del Niño, C. d. l. D. (2021). Observación General núm. 25 relativa a los derechos de los niños en relación con el entorno digital. *Naciones Unidas*.

penal autónomo por primera vez en 2007, en el *Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual* (Convenio de Lanzarote), su identificación como fenómeno de riesgo y patrón de violencia sexual contra la infancia consta en la literatura al menos desde la década de 1980. Estudios criminológicos situados en EE. UU. describieron la existencia de estrategias de seducción y manipulación sexual de niños previas a la agresión directa[5], esto es, como conducta preparatoria de abusos físicos y otros delitos sexuales.

Inicialmente, tanto "grooming" como "seducción" se utilizaban como términos para describir este tipo de conducta no violenta. Con el tiempo, el término *grooming* se ha consolidado como la expresión mayoritaria, utilizada en distintas disciplinas y también en el contexto hispanohablante, para referirse a las tácticas de contacto y manipulación emocional y psicológica de adultos a menores con fines sexuales. En 2016, el documento autorizado *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales* (Directrices de Luxemburgo), identificó el *grooming* como un término equivalente a los delitos de "proposiciones a menores" y de "embaucamiento de menores" con fines sexuales, previstos respectivamente en el Convenio de Lanzarote (2007) y en la *Directiva 2011/93/UE sobre la lucha contra el abuso sexual infantil.* Sin embargo, ha sido necesario esperar hasta 2024 para que el término *grooming* fuera utilizado por primera vez de forma expresa en un instrumento jurídico internacional: la *Convención de las Naciones Unidas contra la Ciberdelincuencia*, donde aparece en su versión en inglés y se traduce al español como 'captación'. Lingüísticamente, el término *grooming* tiene un significado general relacionado con la preparación para una actividad, y otro específico en el ámbito de la protección de la infancia, que designa una forma particular de abuso sexual: el proceso por el que un adulto establece una relación de confianza con un menor con el objetivo de cometer un abuso u otra actividad sexual[6]. Aunque las conductas del grooming pueden darse también en entornos físicos, como el ámbito familiar o institucional, la literatura académica ha vinculado el término especialmente con el entorno digital[7], si bien en este contexto la expresión *grooming digital* se propone como más adecuada[8]. Por otra parte, aunque el objetivo del agresor es preparar al menor para una actividad sexual ello no implica necesariamente contacto físico ni

[5] Burgess, A. W., & Hartman, C. R. (2018). On the origin of grooming. *Journal of Interpersonal Violence*, *33*(1), 17-23.

[6] Greijer, S., & Cruz, T. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales. *ECPAT International. Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes. Recuperado a partir de http://luxembourgguidelines.org/es*.

[7] McAlinden, A.-M. (2012). *'Grooming'and the Sexual Abuse of Children: Institutional, Internet, and Familial Dimensions*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199583720.001.0001

[8] Lorenzo-Dus, N. (2023). *Digital Grooming: Discourses of Manipulation and Cyber-crime*. Oxford University Press.

violencia directa. En su evolución más reciente, los delitos sexuales contra menores pueden cometerse exclusivamente en línea. Ello configura al *grooming digital* como una modalidad de abuso sexual sin contacto, que en español se describe con el término "acoso sexual" de menores en línea. El *Diccionario de la Lengua Española* ha incorporado el anglicismo *grooming* definiéndolo ya en su sentido específico y digital como ciberacoso sexual de menores. En su dimensión digital, y respecto a los videojuegos, el fenómeno del ciberacoso sexual de menores se analiza dentro del marco más amplio de los riesgos digitales que afectan a los menores, conocido como enfoque de las "4C": riesgos de Contenido (relativos a acceso a material inapropiado), de Contacto (relativos a comunicación de un tercero con un menor con intención de causarle daño), de Conducta (comportamientos perjudiciales entre menores/iguales) y de Contrato (prácticas comerciales abusivas o manipulativas)[9]. Como amenaza digital, el ciberacoso sexual de menores se entiende como una manifestación concreta de "riesgo de contacto": los delincuentes utilizan las plataformas y redes sociales para tomar contacto con los menores y, más o menos progresivamente, engañarles, embaucarles, y captarles con fines sexuales. Según la Relatora especial de las Naciones Unidas sobre la venta y la explotación sexual de niños, niñas y adolescentes:

> "Al comunicarse en línea, el *groomer*, aunque no esté físicamente presente, manipula al menor y puede inducirlo a presenciar, ver o participar en la producción de material sexual en línea. Este material puede ser visualizado por el agresor y utilizado como material de abuso infantil. Una vez difundido en Internet, resulta extremadamente difícil eliminarlo, lo que genera un abuso continuo y un daño duradero al niño. En algunos casos, también puede llevar a que el adulto organice un encuentro físico con el menor con el propósito de cometer delitos sexuales en su contra"

Aunque las tácticas de *grooming* no son nuevas, Internet y las tecnologías digitales ofrecen nuevas oportunidades a los depredadores sexuales. En particular, el anonimato que ofrece el contexto digital permite a los usuarios ocultar su identidad y circunstancias personales, como la edad o el sexo. Esta opacidad dificulta la identificación inicial del agresor permitiendo que contacte y desarrolle el proceso de manipulación del menor, presentando desafíos en su detección y reacción temprana. El fenómeno del *grooming* digital ha ido evolucionando, adaptándose al desarrollo tecnológico: desde la utilización de las TICs en su forma más rudimentaria (mensajería instantánea de MSN Messenger o salas de chat en línea de Yahoo) para establecer comunicación con el menor con vistas a un futuro encuentro presencial en el que se llevaría a cabo el abuso sexual; hasta la manipulación e inducción para que el menor se auto-grabe, generando imágenes y

[9] del Niño, C. d. l. D. (2021). Observación General núm. 25 relativa a los derechos de los niños en relación con el entorno digital. *Naciones Unidas*.

videos de carácter sexual (material de abuso sexual infantil, o MASI) sin abandonar el entorno digital (redes sociales, videojuegos, sistemas de mensajería, etc); o la más reciente manifestación en la que el uso de inteligencia artificial permite a los agresores crear material sexual infantil falso o interactuar con menores a través de sistemas automatizados. Las plataformas de juego virtual constituyen un canal tecnológico más, aunque algunas de sus características las hacen especialmente vulnerables a las prácticas de grooming[10]. Ello se debe a que es una modalidad tecnológica que combina anonimato y posibilidad de uso de identidades falsas (estimulado, en ocasiones, por la propia plataforma como parte de la dinámica del juego); presencia masiva de menores (en rangos de edad diversos); interacción lúdica abierta y espontánea (en algunos juegos se parte de la regla de jugar con extraños como un ejercicio colaborativo entre personajes, por ejemplo, mediante el uso de avatares, para lo cual integran servicios de chat o voz); y una escasa o deficiente supervisión parental (ya sea por desconocimiento de los riesgos o por una excesiva confianza derivada del carácter lúdico del entorno).

Ciertamente, ello no significa que todos los videojuegos online sean "juegos peligrosos" *per se* sino que el riesgo depende del uso que pueda hacerse de sus funcionalidades en ausencia de controles eficaces. En este sentido, la gran mayoría de los títulos que permiten la participación de menores incluyen configuraciones de control parental (tiempo de uso, deshabilitado de funciones como compras o mensajes directos, administración de solicitudes de amistad, filtros de lenguaje ofensivo, etc.)[11]. Sin embargo, estas medidas de control no siempre se activan o los padres y tutores las autorizan sin comprender plenamente su funcionamiento[12], lo que evidencia una brecha de formación en educación digital. Todo ello convierte a los videojuegos multijugador en línea, en concreto aquellos con funcionalidades de comunicación abierta, en canales especialmente propicios para la captación de menores -fase inicial del grooming-, ya que el contacto con desconocidos suele percibirse como una dinámica de juego más. Los agresores lo saben y aprovechan esa normalización para aproximarse al menor en aquellos juegos o plataformas de juego que permiten la interacción directa entre jugadores, incluidos sistemas de chat privado, herramientas de audio y video, y mecanismos para compartir ficheros integrados en el juego[13]. A ello se suman otras características frecuentes en los

[10] Rojas, J. (2024). *Child Grooming en videojuegos en línea: Un análisis de la ciberdelincuencia y la protección de los niños en América Latina*. Programa Líderes 2.0 del Registro de Direcciones de Internet de América Latina y Caribe (LACNIC).

[11] de Nova Labián, A. (2025). Determinación y análisis del sistema de responsabilidad y obligaciones de las plataformas de videojuegos en el Reglamento de servicios digitales. *Estudios de Deusto: revista de Derecho Público*, *73*(1), 119-156.

[12] Families are Europe'e Treasure (FAET). (2023). *The European Parliament calls for better child protection in online video games environment*. https://www.fafce.org/the-european-parliament-calls-for-better-child-protection-in-online-video-games-environment/

[13] Ministerio de Juventud e Infancia de España. (2024, septiembre 12). Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Diagnóstico sobre los

videojuegos, como la hipersexualización de contenidos o el uso de *dark patterns* (patrones de diseño que inducen comportamientos o decisiones no plenamente conscientes), que pueden actuar como factores coadyuvantes en la fase de manipulación y embaucamiento del menor hacia la actividad sexual. Finalmente, en los últimos años, diversas iniciativas regulatorias en el ámbito de la Unión Europea parten de la constatación de deficiencias estructurales y mecanismos de supervisión interna insuficientes en la industria del videojuego en materia de protección infantil, y abogan por reforzar la responsabilidad de las plataformas de juego y demás proveedores de servicios digitales en la detección y protección frente a la delincuencia sexual infantil en línea. Por un lado, la *Propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores* (2022)[14], todavía en proceso legislativo, otorga a los prestadores de servicios digitales, incluidos los servicios de juego, un papel preponderante imponiéndoles obligaciones de evaluación de riesgos de uso indebido sus servicios para abusar sexualmente de menores en línea, y, en su caso, de detección proactiva y denuncia de conductas de embaucamiento de menores (grooming) así como la eliminación y bloqueo de material de abuso sexual infantil. Por su parte, la *Resolución del Parlamento Europeo sobre la protección de los consumidores en los videojuegos en línea* (2023)[15] reconoce los riesgos específicos que estos entornos suponen para los menores y llama a reforzar la autorregulación de la industria mediante controles parentales eficaces, una mayor transparencia y diseños responsables desde la fase del desarrollo. La resolución reconoce la utilidad de los sistemas de clasificación por edades (PEGI) que incluyen los videojuegos como recomendación al consumidor, pero otros agentes alertan que se trata de mecanismos voluntarios y meras guías que no incorporan ningún método de verificación que limite, *de facto*, el acceso para menores en edades no recomendadas[16]. Por el momento, a falta de aplicación de estas iniciativas aún en tramitación, la Ley de Servicios Digitales (Reglamento UE 2022/2065)[17] constituye hoy el marco operativo en la UE que fija el "estándar de diligencia" de las plataformas en línea accesibles a menores, como es el caso de los videojuegos en línea[18]. Entre otras obligaciones de diligencia debida y

entornos digitales y su impacto en la protección de niños, niñas y adolescentes.

[14] Parlamento Europeo y Consejo de la Unión Europea. (2022, mayo 11). *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores*. COM(2022) 209 final, 2022/0155 [COD].

[15] Parlamento Europeo. (2023, enero 18). *Resolución del Parlamento Europeo sobre la protección de los consumidores en los videojuegos en línea: Un enfoque a escala del mercado único europeo (2023/C 214/0).*

[16] Ministerio de Juventud e Infancia de España. (2024, septiembre 12). Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Diagnóstico sobre los entornos digitales y su impacto en la protección de niños, niñas y adolescentes.

[17] Parlamento Europeo y Consejo de la Unión Europea. (2022, octubre 19). *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, relativo a un mercado único de servicios digitales (Ley de Servicios Digitales) y por el que se modifica la Directiva 2000/31/CE*. DOUE, L 277/1, 27.10.2022.

[18] de Nova Labián, A. (2025). Determinación y análisis del sistema de responsabilidad y obligaciones de las plataformas de videojuegos en el Reglamento de servicios digitales. *Estudios de Deusto: revista de Derecho Público*, *73*(1), 119-156.

responsabilidades, este reglamento obliga a las plataformas en línea a adoptar medidas apropiadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea (art. 28), y la Comisión Europea ha concretado en 2025 qué entiende por "medidas adecuadas" para valorar su cumplimiento en el documento de Directrices sobre la aplicación del artículo 28(Comisión Europea, 2025, octubre 10). Dichas Directrices señalan, entre otras medidas, la necesidad de establecer controles de contacto y visibilidad por defecto, mecanismos de denuncia adaptados a menores, y protocolos específicos de moderación y formación del personal frente a riesgos de captación o grooming. Volveremos a ellas más adelante. En este contexto, se realiza la actividad empírica que se presenta a continuación, destinada a analizar cómo se comporta un videojuego multijugador masivo en línea, *Fortnite*, frente a indicios de riesgos de captación y ciberacoso sexual infantil (grooming) y a los mecanismos reporte y respuesta temprana implementados por la plataforma, con el fin de valorar la eficacia y las limitaciones de las medidas implementadas por la plataforma e identificar posibles áreas de mejora.

II. **Metodología**

Para la ejecución de la metodología se han utilizado dos identidades supuestas, optando por el uso de la etnografía virtual encubierta como metodología de investigación; la etnografía virtual encubierta permite llevar a cabo una interacción parametrizada con los participantes del videojuego y salvaguardar la integridad de los investigadores ante posibles reprimendas derivadas del proceso de investigación. A continuación, se detalla el proceso diseñado para interactuar en *Fortnite* mediante las identidades supuestas generadas a tal fin.

1. ***Campo de Estudio***

El proceso de etnografía virtual encubierta da comienzo tras el acceso a la modalidad de *Party Royale* incluida en el videojuego *Fortnite*; esta modalidad permite el uso de chat grupal e individual para establecer comunicación con usuarios sin necesidad de utilizar dispositivos de audio; por otro lado, *Party Royale* facilita un ambiente distendido para que los participantes puedan relacionarse entre sí lejos de la dinámica habitual del videojuego. Se accede a *Fortnite* en horas aleatorias entre las 20:00 h y las 24:00 h, durante un período de 31 días no consecutivos.

2. ***Características de las Identidades Supuestas***

2.1. *Identidad Supuesta de Cibervíctima*

La creación y exposición de una identidad supuesta de cibervíctima tiene como

objetivo recopilar información relacionada con casos de ciberacoso en el entorno de *Fortnite* mediante la interacción con otros participantes. La identidad supuesta de cibervíctima se corresponde a la de un usuario con una edad de 15 años; la delimitación de la edad es fundamental ya que estudios como el elaborado por Montiel[19], señalan una alta prevalencia de ciberacoso sexual en usuarios con edades comprendidas hasta los 17 años, mientras que, por su parte, investigadores como Ortega-Barón y otros[20] determinan necesario limitar el alcance de sus investigaciones hasta los 15 años. Obedeciendo a la modalidad pasiva (*véase apartado Rol adoptado en las interacciones*), la identidad supuesta ha de contar con una edad que resulte atractiva ante un potencial escenario de abordaje, mientras que, desde el prisma de la modalidad activa (véase apartado *Rol adoptado en las interacciones*), situarse en el rango de edad de las víctimas ayuda a que se genere un vínculo de confianza con estas, permitiendo obtener la información esperada en el proceso de interacción. Por otro lado, se ha determinado construir las características de la supuesta cibervíctima en torno al sexo femenino; esta elección responde a un análisis exhaustivo de videojuegos llevado a cabo por Lynch y otros[21] en el cual encontraron frecuentes narrativas sexistas que cosificaban a los personajes femeninos; así mismo, existen diversos estudios que apuntan que las mujeres son marginadas y acosadas cuando consumen videojuegos debido a su género, y esto podría explicar por qué las mujeres consumen menos videojuegos que los hombres[22]. Finalmente, y al objeto de mantener el mismo discurso a lo largo de tiempo, se han incluido una serie de datos personales dentro de la ficha de la identidad supuesta que abarcan desde el peso, la altura, colores de ojos, barrio de nacimiento, nombre y apellidos, colores favoritos, comidas favoritas, o situación familiar actual.

2.2. *Identidad Supuesta de Ciberacosador*

La creación de una identidad supuesta de ciberacosador tiene como objetivo único objetivo la interacción con la identidad supuesta de la cibervíctima, esto es, no se utiliza bajo ningún concepto para interactuar con el resto de los usuarios presentes en el videojuego. Con ello, se pretende evaluar, desde el punto de vista de

[19] Juan, I. M. (2016). Cibercriminalitat social juvenil: la xifra negra. *IDP. Revista de internet, derecho y política*(22). https://doi.org/10.7238/idp.v0i22.2972

[20] Ortega-Barón, J., Machimbarrena, J. M., Caba-Machado, V., Díaz-López, A., Tejero-Claver, B., & González-Cabrera, J. (2023). Solicitation and sexualized interactions of minors with adults: Prevalence, overlap with other forms of cybervictimization, and relationship with quality of life. *Psychosocial intervention*, *32*(3), 155. https://doi.org/10.5093/pi2023a15

[21] Lynch, T., Tompkins, J. E., Van Driel, I. I., & Fritz, N. (2016). Sexy, strong, and secondary: A content analysis of female characters in video games across 31 years. *Journal of communication*, *66*(4), 564-584. https://doi.org/https://doi.org/10.1111/jcom.12237

[22] Valentowitsch, J. (2024). Does sex sell? Gender representation, sexualization, and violence on video game covers and their impact on sales. *Journal of Business Strategies*, *41*(1), 27-42.

una potencial cibervíctima, que tan efectivos son los mecanismos aplicados a una cuenta que ha sido denunciada por ciberacoso. La identidad supuesta ha sido configurada teniendo en cuenta que gran parte de los ciberacosadores de menores son hombres Wachs y otros[23], con una edad promedio de 35 años[24].

3. *Roles Adoptados en las Interacciones*

Para el presente estudio se ha utilizado un triple enfoque en el proceso de interacción.

- Modo activo: El objetivo de esta modalidad es lograr interacciones con potenciales víctimas de ciberacoso; para ello, se procede a exponer en un chat general o privado un presunto caso de ciberacoso, buscando la complicidad de aquellos que hayan vivido una experiencia similar. Se pretende con ello hallar potenciales víctimas que contribuyan a evaluar la criticidad del videojuego dentro del contexto del ciberacoso a menores. La selección de las potenciales víctimas se basa en la respuesta ofrecida por los participantes, o lo que es lo mismo, cuando un usuario reacciona ante la exposición del presunto caso de ciberacoso, se inicia una conversación privada con el mismo. Finalmente, se procede a realizar un conjunto de preguntas que permiten obtener información para nutrir las variables esperadas.
- Modo pasivo: El objetivo de esta modalidad es el fijar la atención de potenciales agresores hacia la identidad supuesta; bajo esta premisa, la identidad supuesta inicia las partidas presentándose al conjunto de jugadores con su edad y nombre, pero en ningún momento se realizan acercamientos a un usuario en concreto, esperando así que el proceso de abordaje sea lo más natural posible.
- Modo test: Mediante esta modalidad se pretende acumular mensajes ofensivos provenientes de la identidad supuesta de ciberacosador con destino a la identidad supuesta de cibervíctima para luego proceder a realizar una denuncia mediante los canales oficiales de Fortnite. El objetivo final es evaluar la efectividad del proceso de notificación y reacción ante casos de ciberacoso.

Por último, cabe aclarar que, si bien se han empleado las tres modalidades, el modo test ha tenido un recorrido menor dado su objetivo inminente; sin embargo, y a lo que al modo activo y pasivo se refiere, han sido ejecutados en días alternos durante la ejecución del trabajo empírico.

---

[23] Wachs, S., Jiskrova, G. K., Vazsonyi, A. T., Wolf, K. D., & Junger, M. (2016). A cross-national study of direct and indirect effects of cyberbullying on cybergrooming victimization via self-esteem. *Psicologia educativa*, *22*(1), 61-70. https://doi.org/10.1016/j.pse.2016.01.002

[24] Riberas-Gutiérrez, M., Reneses, M., Gómez-Dorado, A., Serranos-Minguela, L., & Bueno-Guerra, N. (2024). Online grooming: Factores de riesgo y modus operandi a partir de un análisis de sentencias españolas. *Anuario de Psicologia Juridica*, *34*(1), 119-131. https://doi.org/10.5093/apj2023a9

4. *Taxonomía del Discurso de Odio*

Basándonos en la taxonomía del odio establecida por Fernando Miró en su artículo Taxonomía de la comunicación violenta y el discurso del odio en Internet[25], se procede a establecer la siguiente escala para medir el nivel de intensidad del discurso ofensivo ante situaciones de ciberacoso en videojuegos:

- Other Attack-Non Sexual Related: Bajo esta categoría se encuadran casos de ciberacoso relacionados con discurso ofensivo o de mal gusto sin ser necesariamente ciberacoso sexual.
- Attack on Dignity-Medium: palabras vulgares referentes a partes del cuerpo. Discurso que atenta contra la intimidad sexual. Se diferencia en esta escala ataques relacionados con ciberacoso sexual y ataques relacionados con *grooming digital*.
- Attack on Dignity-High: insultos directos o palabras referentes al acto sexual. Discurso que atenta contra la intimidad sexual. Se diferencia en esta escala ataques relacionados con ciberacoso sexual y ataques relacionados con *grooming digital*.
- Threat: discurso violento agravado que atenta contra la integridad y seguridad. Se diferencia en esta escala ataques relacionados con ciberacoso sexual y ataques relacionados con *grooming digital*.

5. *Variables de Estudio*

Bajo el siguiente conjunto de variables, se ha procedido a almacenar temporalmente los datos obtenidos mediante interacción con usuarios de Fortnite:

- Detección de Víctimas.
  - ID: Identificador auto-incremental.
  - Date: Fecha de la interacción.
  - Age: Edad de la supuesta víctima.
  - Gender: Género de la supuesta víctima.
  - Evidence: Mensaje textual de la potencial víctima dónde se refleja el caso de ciberacoso.
  - Scale: Asignación de nivel de agresividad en el discurso, basado en una taxonomía de mensajes agresivos que atentan contra la dignidad de las personas.
  - Abuse report: valor booleano.
  - Mesure: acciones tomadas contra el usuario que ha sido reportado.
- Detección de Ciberacosadores.
  - ID: Identificador auto-incremental.

[25] Llinares, F. M. (2016). Taxonomía de la comunicación violenta y el discurso del odio en Internet. *IDP. Revista de internet, derecho y política*(22), 82-107.

- Date: Fecha de la interacción.
- Age: edad del potencial ciberacosador.
- Gender: Género del ciberacosador.
- Evidence: mensaje textual del ciberacosador dónde se reflejen indicios de ciberacoso.
- Scale: asignación de nivel de agresividad en el discurso, bajado en una taxonomía de mensajes agresivos que atentan contra la dignidad de las personas.

- Interacciones Totales.
  - ID: Identificador auto-incremental.
  - Gender: Género del usuario.
- Intentos de Interacciones.
  - ID: Identificador auto-incremental.

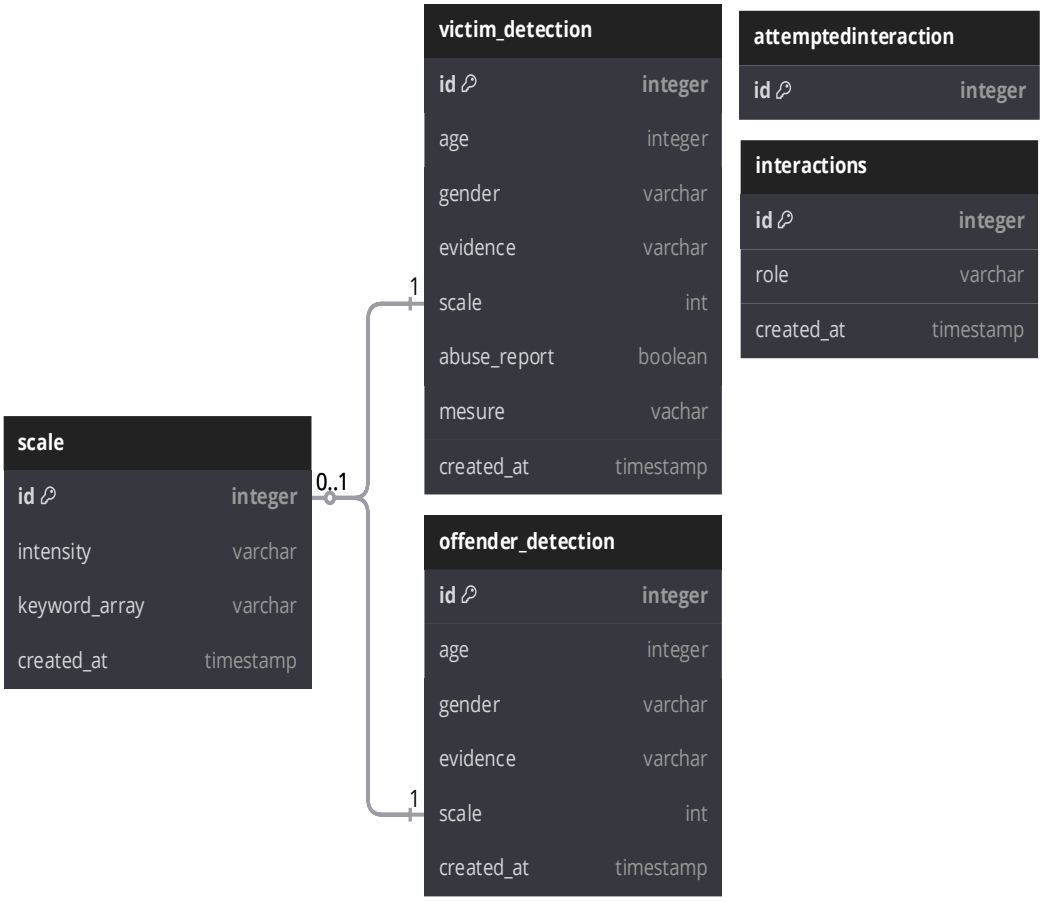

Figura 1: Database

6. ***Fichas Etnográficas***

Finalmente, procedió a generar una ficha de etnografía virtual por cada participante, diferenciado las interacciones con víctimas de ciberacoso de las interacciones relacionadas con potenciales ciberacosadores:

Tabla 1: Ficha de Etnografía Virtual Relacionada con Víctimas de Ciberacoso

Parámetro	Ejemplo
ID	ID001
Date	01/02/2025
Evidence	Me: Have u experienced something similar? Victim: i do it sometimes too.
Age	12
Gender	Female
Scale	1
Abuse Report	Yes
Mesure	Reported several times to users via the 'reporting player' option, it indicates that this measure works.
Additional inputs	On 01/02, in our active mode, the user is asked about an alleged case of cyber harassment and how we should report it, she comments that she has had to report it on several occasions but does not indicate if it was for sexual harassment.

Fuente: *Elaboración propia.*

Tabla 2: *Ficha de Etnografía Virtual Relacionada con Ciberacosador*

Parámetro	Ejemplo
ID	ID001
Date	01/02/2025
Evidence	Offender: ***** (asterisks are censorship) Me: You can't tell me that…
Age	31
Gender	Male
Scale	4
Additional inputs	Potential approaching of user for sexual purposes, when the age of the fake victim is known, the user retracts and stops sending racy messages.

Fuente: *Elaboración propia.*

III. **Ética de Investigación**

Mediante la ejecución metodológica se ha evitado la recopilación de datos que puedan conducir a la identificación de los participantes de las interacciones (véase apartado *Variables de estudio*), asegurando con ello que la presente investigación no afecta a la privacidad de los usuarios en Fortnite. Así mismo, el almacenamiento y la retención de datos relativo a los usuarios se encuentra limitado al proyecto de investigación, procediendo a la debida destrucción de estos una vez concluida su finalidad.

IV. **Resultados**

1. ***Resultados Correspondientes al Modo Activo***

Mediante la metodología definida con anterioridad, se ha interactuado con total

de *n=50* usuarios durante 31 días repartidos en 3 meses, de los cuales un amplio conjunto (*n=25*) han respondido a las peticiones de amistad o mensajes iniciales generando con ello interacciones completas (véase Tabla 3).

Tabla 3: *Interacciones Dataset*

Id	Gender
1	Female
2	Female
3	Female
4	Female
5	Male
6	Male
7	Female
8	Female
9	Female
10	Female
11	Female
12	Female
13	Male
14	Male
15	Male
16	Male
17	Female
18	Female
19	Male
20	Male
21	Female
22	Female
23	Unknown
24	Male
25	Unknown

Fuente: *Elaboración propia.*

Del total de interacciones completas, *n=11* se corresponden a usuarios que han sido víctimas de ciberacoso, esto es, un 40,74% sobre el total de interacciones, siendo el género femenino el más representativo con un 51,85% de presencia en los casos registrados. En cuanto a la edad de las supuestas víctimas de ciberacoso, *n=3* usuarios presentan edades indeterminadas, mientras que *n=5* usuarios se corresponden a víctimas menores de edad (=< 18 años) frente a *n=3* usuarios adultos (>18 años); del conjunto de usuarios menores, un 60% (*n=3*) contaba con una edad igual o inferior a 16 años en el momento de la interacción (véase Figura 2).

Tabla 4: Víctimas Dataset

Id	Age	Gender	Scale	Abuse_Report
1	12	Female	1	Yes
2	17	Female	1	Yes
3	NULL	Female	2	Yes
4	21	Male	1	Yes
5	NULL	Female	1	Yes
6	16	Female	1	Yes
7	14	Female	5	Yes
8	20	Female	1	Yes
9	26	Female	2	Yes
10	17	Female	1	No
11	NULL	Unknown	2	Yes

Fuente: *Elaboración propia.*

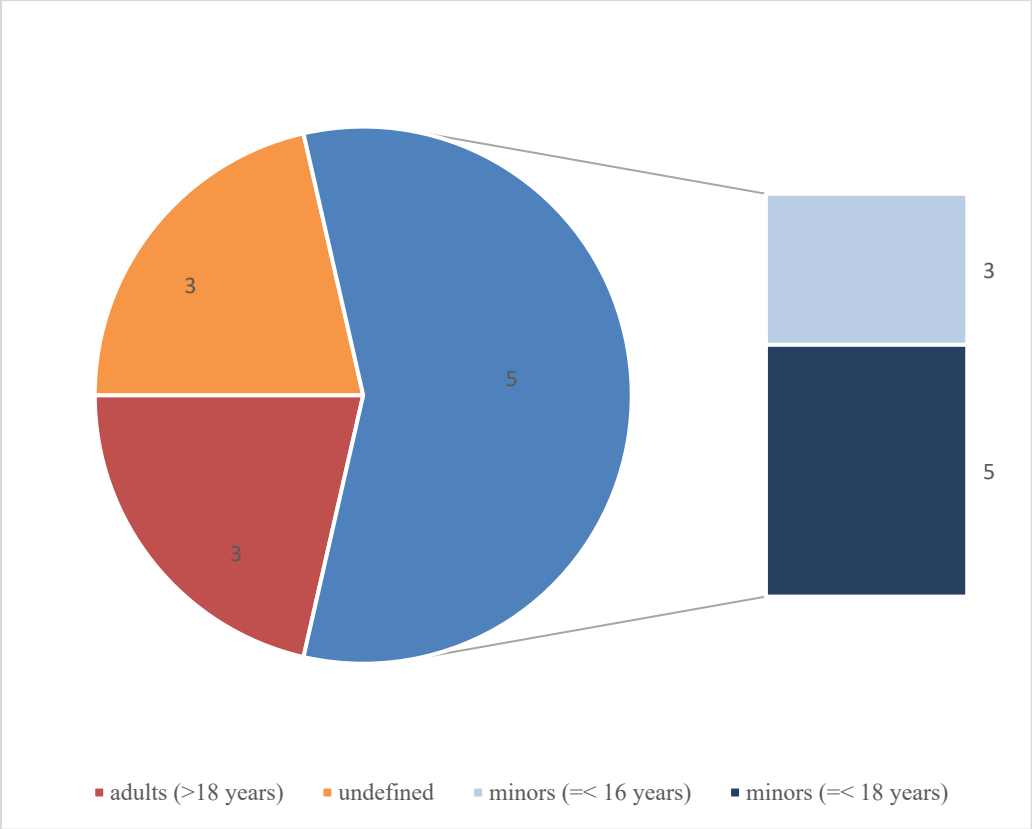

Figura 2: Number of Victims by Age

Finalmente, del conjunto de usuarios que han sufrido episodios de ciberacoso, *n=7* no especifican la intensidad del discurso empleada por el ciberacosador, ante lo cual se atribuye la escala más baja dentro discurso de odio (escala 1); por otra parte, *n=4* usuarios han reportado algún tipo de acoso sexual, correspondiéndose uno de estos a un menor de 16 años (véase Figura 3).

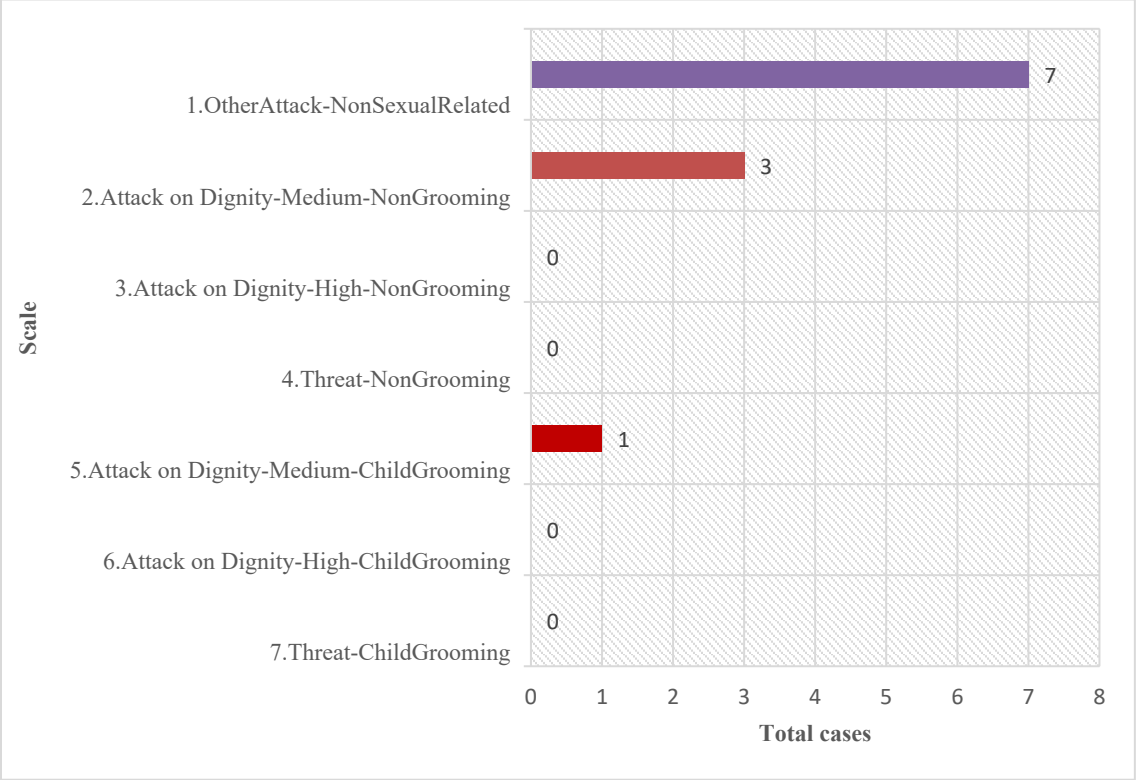

Figura 3: Hate Speech Scale

2. ***Resultados Correspondientes al Modo Pasivo***

En lo relativo a la detección de usuarios que hayan ejercido ciberacoso ante la supuesta cibervíctima, únicamente se ha registrado una interacción. El usuario ciberacosador cuenta con una edad de 20 años en el momento de la interacción y emplea un lenguaje mal sonante que resulta imposible de categorizar al encontrarse totalmente censurado por el videojuego.

3. ***Resultados Correspondientes al Modo Test***

Mediante el registro de la interacción y consecuente proceso de denuncia entre la supuesta cibervíctima y el supuesto ciberacosador, se han podido recoger los siguientes indicadores en una bitácora:

- Día 07-02: El usuario ciberacosador agrega a la supuesta cibervíctima por búsqueda de usuarios en la misma zona geográfica, éste le escribe por chat supuesta cibervíctima en tono amistoso y le propone de verse en el juego; la supuesta cibervíctima lo añade a su grupo para invitarle a la partida en la modalidad Party Royale, el ciberacosador comienza a dialogar subiendo gradualmente el tono del discurso mediante el uso de palabras mal sonantes; finalmente, la supuesta cibervíctima abre un reporte de denuncia (véase Figura 4) que genera automáticamente un ticket asociado (véase Figura 5), instantáneamente, el usuario ciberacosador deja de poder chatear con la

supuesta cibervíctima aunque esta se encuentra online, denotando una primera medida reactiva más suficiente por parte de Fortnite.

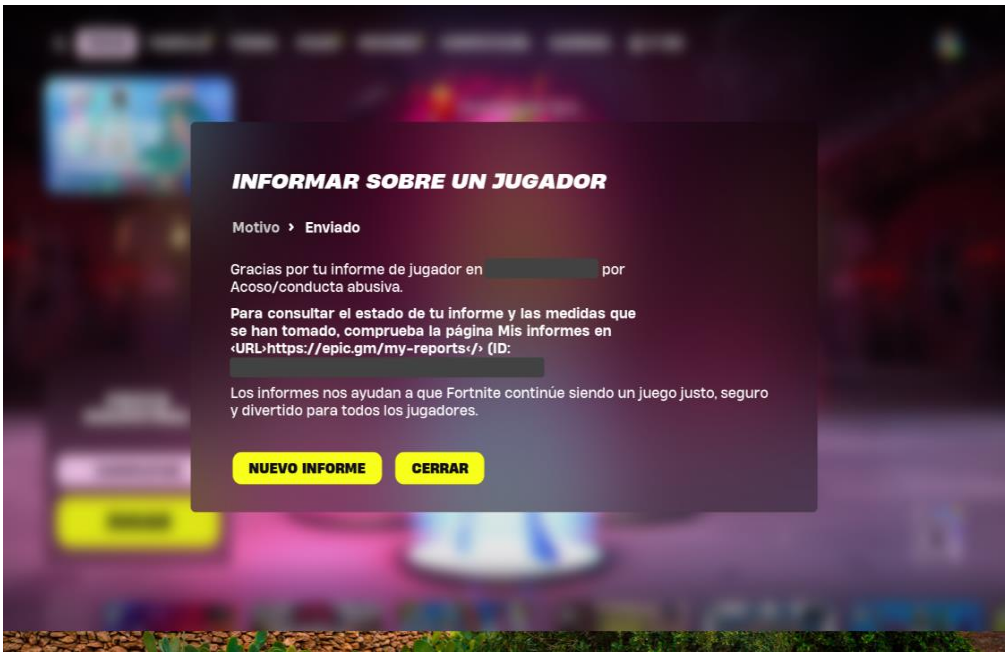

Figura 4: Fortnite Reporting

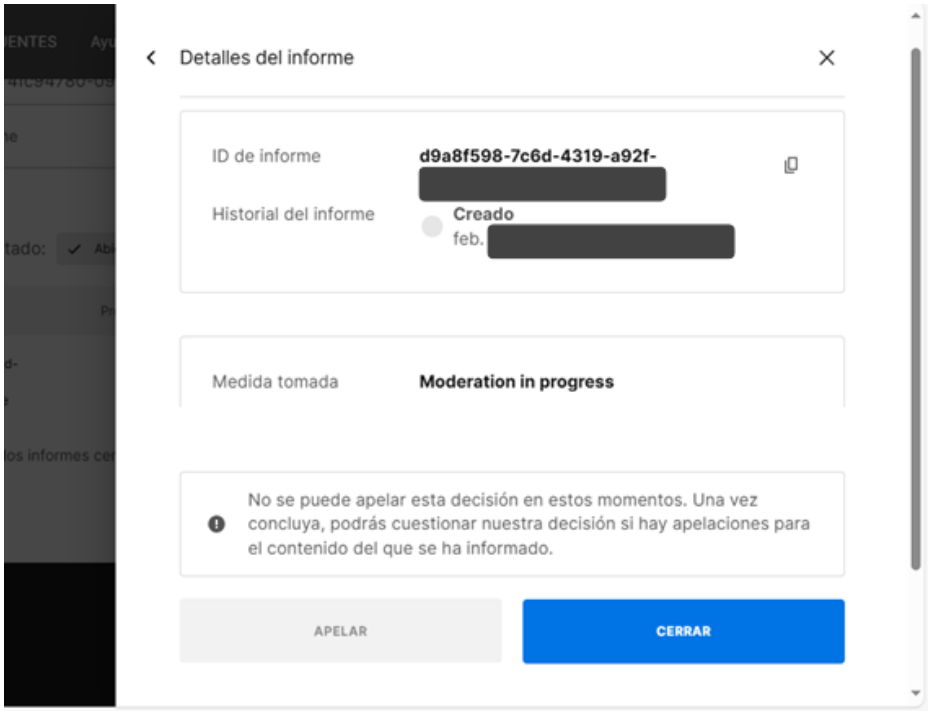

Figura 5: Fortnite Reporting Web

- Día 08-02: Transcurridas las primeras 24 h desde la denuncia, se comprueba que el usuario denunciado sigue sin poder chatear con la supuesta cibervíctima y esta última ya no figura como "amigo" conectado (aunque sí

está online); sin embargo, el usuario ciberacosador puede seguir jugando y abriendo chats con otros usuarios, aunque esto se encuentra fuera del alcance para evitar que la investigación pueda estar asociada con conductas delictivas. Todo ello demuestra que no hay mecanismos preventivos suficientes para evitar que el supuesto ciberacosador replique el discurso ofensivo con otros usuarios.

- Día 09-02: Transcurridas las primeras 48 h desde la denuncia, se accede a la cuenta de Fortnite de la supuesta cibervíctima para conocer el estado actual de la denuncia, y se constata que el ticket asociado se encuentra en estado "abierto" y sin resolver; por su parte, el supuesto ciberacosador sigue pudiendo acceder a Fortnite.

Para comprobar que no se ha impuesto ningún tipo de restricción a nivel de hardware que deniegue la comunicación con la supuesta cibervíctima, se procede a añadir una nueva fase que consiste en crear un segundo usuario para el perfil del supuesto ciberacosador; en este sentido, el nuevo usuario ha sido generado por el supuesto ciberacosador, buscando así otra vía de acoso a la supuesta cibervíctima mediante la evasión de las medidas de seguridad aplicadas a la cuenta; finalmente, la nueva supuesta identidad registrada por el ciberacosador le permite volver a acceder a la cibervíctima vía Chat, de ello se deduce que Fortnite únicamente ha aplicado medidas de restricción a nivel usuario, pero no a nivel de harware. Cabe resaltar, no obstante, que Fortnite dispone de un sistema Anti-Cheat que permite aplicar restricciones de acceso basadas en Hardware, un sistema que responde de manera efectiva cuando un usuario infringe las normas del juego, por ejemplo, si se detecta un uso anómalo mediante VPN o envíos de paquetes modificados al servidor; sin embargo, y ante casos de ciberacoso, se ha podido evidenciar que el sistema Anti-Cheat no ha sido aplicado, permitiendo al usuario ciberacosador seguir accediendo a su víctima bajo una nueva identidad.

- Día 12-02: Transcurridos cinco días desde la denuncia, el supuesto ciberacosador aún no ha sido eliminado o contenido en sistema, pudiendo acceder a su cuenta con normalidad. Y el ticket asociado con la denuncia continúa en estado pendiente de resolver.
- Día 14-02: Transcurrida una semana desde la denuncia, el supuesto ciberacosador aún no ha sido eliminado o contenido en sistema, pudiendo acceder a su cuenta con normalidad. Y el ticket asociado con la denuncia continúa en estado pendiente de resolver.
- Día 21-02: Transcurridas dos semanas desde la denuncia, el supuesto ciberacosador aún no ha sido eliminado o contenido en sistema, pudiendo acceder a su cuenta con normalidad. Y el ticket asociado con la denuncia continúa en estado pendiente de resolver.
- Día 21-03: Transcurrido un mes desde la denuncia, el supuesto ciberacosador

aún no ha sido eliminado o contenido en sistema, pudiendo acceder a su cuenta con normalidad. Y el ticket asociado con la denuncia continúa en estado pendiente de resolver.

V. **Discusiones y Principales Conclusiones**

El análisis de los resultados obtenidos en el modo activo revela una interacción sostenida con 50 usuarios a lo largo de tres meses, de los cuales la mitad (*n=25*) respondieron de forma efectiva, generando interacciones completas. De estas, el 40,74% (*n=11*) correspondieron a situaciones de ciberacoso, con un predominio de víctimas de género femenino (51,85%). En esta dirección, y si bien recientes investigaciones como la publicada por Reneses *et al* [26] señalan el aislamiento social, la curiosidad sexual o la mala comunicación familiar, como principales mecanismos de vulnerabilidad explotados por los agresores, el presente trabajo permite complementar dicho enfoque cualitativo al demostrar que los sujetos activos no solo buscan un contacto verbal o simbólico, sino que también aprovechan las dinámicas de interacción regular (interacciones completas) para progresar gradualmente en su discurso; todo ello fortalece la plausibilidad de los modelos de grooming que incluyen manipulación escalable. Adicionalmente, se identificó que cinco de las víctimas eran menores de edad, siendo tres de ellas menores de 16 años, lo que resalta la especial vulnerabilidad de este grupo etario en entornos digitales; esta observación concuerda con lo expuesto por Whittle *et al.*[27] ya que sugerían a los adolescentes como grupo más vulnerable al *grooming digital*. Además, cuatro de los casos incluyeron reportes de acoso sexual, uno de ellos dirigido a una menor, lo que evidencia la gravedad del problema y la necesidad de reforzar los mecanismos de protección específicos para menores. Este análisis relativo a la incidencia en menores en juegos online ha sido objeto de estudio en otros informes sistemáticos recientes como el conducido por WeProtect[28], en el cual se especifica una concentración elevada de menores en Minecraft y Roblox. Por otro lado, en el modo pasivo, se logró detectar solo un caso claro de comportamiento de ciberacoso. El agresor, un usuario de 20 años, utilizó un lenguaje inapropiado que fue censurado automáticamente por el sistema del videojuego, impidiendo su categorización adecuada. Esta detección sugiere importantes limitaciones para identificar conductas de acoso, lo que refuerza la

[26] Reneses, M., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2024). "He flattered me". A comprehensive look into online grooming risk factors: Merging voices of victims, offenders and experts through in-depth interviews. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *18*(4).

[27] Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and violent behavior*, *18*(1), 135-146.

[28] WeProtect. (2022). *Gaming and the Metaverse: The alarming rise of online sexual exploitation and abuse of children within the new digital frontier (Informe).* WeProtect. https://www.weprotect.org/wp-content/uploads/Gaming_and_the_Metaverse_Report_final.pdf

necesidad de estrategias automatizadas y proactivas de monitoreo que no dependan exclusivamente de reportes manuales. Carencias similares en la detección y moderación también han sido reseñadas por Rojas[29], documentando que los filtros y las complejidades de las interacciones dificultan la moderación.

Finalmente, los resultados del modo test evidencian importantes deficiencias en la respuesta institucional del videojuego Fortnite frente al ciberacoso. Aunque se aplicaron medidas inmediatas para restringir el contacto entre agresor y víctima, estas fueron fácilmente evadidas mediante la creación de una nueva cuenta por parte del acosador, demostrando que las sanciones se implementan a nivel de usuario, pero no de hardware. Esta brecha permite que los agresores reincidan sin mayores obstáculos. La persistencia del ticket de denuncia en estado "pendiente" durante más de un mes pone de manifiesto la falta de una gestión eficaz y ágil del sistema de denuncias. Estos hallazgos resultan fundamentales para el estudio y prevención del ciberacoso en menores, ya que aportan evidencia empírica sobre los riesgos reales a los que se enfrentan en entornos lúdicos digitales, así como sobre las fallas de los sistemas actuales de protección, lo que justifica la urgente necesidad de diseñar políticas de seguridad más robustas, reactivas y preventivas, que incluyan medidas específicas por parte de las plataformas en línea. En este sentido, a la luz del estándar de diligencia debida previsto en el artículo 28 del Reglamento de Servicios Digitales, tal y como ha sido desarrollado por las Directrices de la Comisión para su aplicación (2025), los resultados del estudio empírico sugieren que las medidas implementadas por *Fortnite* resultan insuficientes para garantizar un nivel adecuado de protección de los menores frente a riesgos de captación o grooming. Por un lado, si bien el sistema de supervisión interna de la plataforma permite una reacción inmediata ante indicios de actividad ilícita, con el bloqueo temporal del contacto entre víctima y agresor, su impacto es limitado, pues carece de un seguimiento personalizado, con supervisión humana, que verifique el incidente. Además, la permanencia prolongada del ticket de denuncia en estado “pendiente” revela una falta de gestión ágil, lo que en conjunto impide considerar la respuesta como temprana y plenamente eficaz, tal y como exige el artículo 28. Por otro lado, la posibilidad de reapertura de cuentas desde otro dispositivo demuestra la inexistencia de mecanismos efectivos de prevención sostenida del riesgo. Este déficit contraviene el principio de protección por diseño y por defecto, señalado en las Directrices de 2025, que obliga a limitar por configuración automática las posibilidades de contacto y en este caso de reincidencia. Finalmente, la ausencia de información al usuario denunciante y en general, sobre el tratamiento de las incidencias, evidencian un incumplimiento de la

[29] Rojas, J. (2024). *Child Grooming en videojuegos en línea: Un análisis de la ciberdelincuencia y la protección de los niños en América Latina*. Programa Líderes 2.0 del Registro de Direcciones de Internet de América Latina y Caribe (LACNIC).

obligación de transparencia en la gestión de denuncias y rendición de cuentas, que constituye otro de los pilares de la diligencia debida en materia de protección infantil en entornos digitales. En consecuencia, como áreas de mejora se propone reforzar los controles de contacto y visibilidad por defecto, asegurando, en primer término, que los menores no puedan ser contactados por desconocidos sin consentimiento explícito y, en segundo lugar, que se restrinja el contacto con usuarios sobre los que exista una queja o denuncia pendiente. Asimismo, debería implementarse un sistema reactivo de sanciones por parte de la plataforma en línea basado en hardware o dispositivo, que impida la reapertura de cuentas por parte de agresores previamente denunciados. Finalmente, cabe apuntar que otra de las herramientas señaladas en las Directrices se refiere a la cooperación de las plataformas en línea con las autoridades competentes, un aspecto no testado en este estudio pero que también debería desarrollarse para reforzar la rendición de cuentas, así como la confianza y protección de los usuarios.

1. ***Implicaciones y Trabajos Futuros***

- Confirmación de patrones demográficos: los resultados refuerzan la evidencia existente de mayor victimización en mujeres y adolescentes (especialmente entre 15–17 años). Este patrón sugiere la elaboración de estrategias preventivo-educativas enfocadas en esos grupos.
- Atención al ciberacoso sexual infantil: el registro de *Grooming digital* subraya la necesidad de incorporar en el diseño protocolos que aborden la detección y respuesta ante indicios de captación de menores con fines sexuales, tanto por parte de las entidades gubernamentales, como por las entidades educativas, y las fuerzas y cuerpos de seguridad.

Referencias

Burgess, A. W., & Hartman, C. R. (2018). On the origin of grooming. *Journal of Interpersonal Violence*, *33*(1), 17-23.

Comisión Europea. (2025, octubre 10). *Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065, DOUE Comunicación C/2025/5519*.

de Nova Labián, A. (2025). Determinación y análisis del sistema de responsabilidad y obligaciones de las plataformas de videojuegos en el Reglamento de servicios digitales. *Estudios de Deusto: revista de Derecho Público*, *73*(1), 119-156.

Del Niño, C. D. L. D. (2011). Observación general No. 13. Derecho del niño a no ser objeto de ninguna forma de violencia. *Ginebra, Suiza: Comité de Defensa del Niño*. https://www.acnur.org/fileadmin/Documentos/BDL/2012/8603.pdf

del Niño, C. d. l. D. (2013). Observación general No 16 (2013) Sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño. *Recuperado de: https://www.right-to-education.org/sites/right-toeducation.org/files/resourceattachments/CRC_Observaci%C3%B3n_general_16_ES_2013.pdf*.

del Niño, C. d. l. D. (2021). Observación General núm. 25 relativa a los derechos de los niños en relación con el entorno digital. *Naciones Unidas*.

Families are Europe'e Treasure (FAET). (2023). *The European Parliament calls for better child protection in online video games environment*. https://www.fafce.org/the-european-parliament-calls-for-better-child-protection-in-online-video-games-environment/

Greijer, S., & Cruz, T. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales. *ECPAT International. Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes. Recuperado a partir de http://luxembourgguidelines.org/es*.

Juan, I. M. (2016). Cibercriminalitat social juvenil: la xifra negra. *IDP. Revista de internet, derecho y política*(22). https://doi.org/10.7238/idp.v0i22.2972

Llinares, F. M. (2016). Taxonomía de la comunicación violenta y el discurso del odio en Internet. *IDP. Revista de internet, derecho y política*(22), 82-107.

Lorenzo-Dus, N. (2023). *Digital Grooming: Discourses of Manipulation and Cyber-crime*. Oxford University Press.

Lynch, T., Tompkins, J. E., Van Driel, I. I., & Fritz, N. (2016). Sexy, strong, and secondary: A content analysis of female characters in video games across 31 years. *Journal of communication*, *66*(4), 564-584. https://doi.org/https://doi.org/10.1111/jcom.12237

McAlinden, A.-M. (2012). *'Grooming'and the Sexual Abuse of Children: Institutional, Internet, and Familial Dimensions*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199583720.001.0001

Ministerio de Juventud e Infancia de España. (2024, septiembre 12). Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. Diagnóstico sobre los entornos digitales y su impacto en la protección de niños, niñas y adolescentes.

Ortega-Barón, J., Machimbarrena, J. M., Caba-Machado, V., Díaz-López, A., Tejero-Claver, B., & González-Cabrera, J. (2023). Solicitation and sexualized interactions of minors with adults: Prevalence, overlap with other forms of cybervictimization, and relationship with quality of life. *Psychosocial intervention*, *32*(3), 155. https://doi.org/10.5093/pi2023a15

Parlamento Europeo. (2023, enero 18). *Resolución del Parlamento Europeo sobre la protección de los consumidores en los videojuegos en línea: Un enfoque a escala del mercado único europeo (2023/C 214/0)*.

Parlamento Europeo y Consejo de la Unión Europea. (2022, mayo 11). *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores*. COM(2022) 209 final, 2022/0155 [COD].

Parlamento Europeo y Consejo de la Unión Europea. (2022, octubre 19). *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, relativo a un mercado único de servicios digitales (Ley de Servicios Digitales) y por el que se modifica la Directiva 2000/31/CE*. DOUE, L 277/1, 27.10.2022.

Reneses, M., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2024). "He flattered me". A comprehensive look into online grooming risk factors: Merging voices of victims, offenders and experts through in-depth interviews. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *18*(4).

Riberas-Gutiérrez, M., Reneses, M., Gómez-Dorado, A., Serranos-Minguela, L., & Bueno-Guerra, N. (2024). Online grooming: Factores de riesgo y modus operandi a partir de un análisis de sentencias españolas. *Anuario de Psicologia Juridica*, *34*(1), 119-131. https://doi.org/10.5093/apj2023a9

Rojas, J. (2024). *Child Grooming en videojuegos en línea: Un análisis de la ciberdelincuencia y la protección de los niños en América Latina*. Programa Líderes 2.0 del Registro de Direcciones de Internet de América Latina y Caribe (LACNIC).

Valentowitsch, J. (2024). Does sex sell? Gender representation, sexualization, and violence on video game covers and their impact on sales. *Journal of Business Strategies*, *41*(1), 27-42.

Wachs, S., Jiskrova, G. K., Vazsonyi, A. T., Wolf, K. D., & Junger, M. (2016). A cross-national study of direct and indirect effects of cyberbullying on cybergrooming victimization via self-esteem. *Psicologia educativa*, *22*(1), 61-70. https://doi.org/10.1016/j.pse.2016.01.002

WeProtect. (2022). *Gaming and the Metaverse: The alarming rise of online sexual exploitation and abuse of children within the new digital frontier (Informe).* WeProtect. https://www.weprotect.org/wp-content/uploads/Gaming_and_the_Metaverse_Report_final.pdf

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and violent behavior*, *18*(1), 135-146.