

HIS PROVIDE ET PRO

Revista

Julio 2026

58

l'enc



tirant
lo blanch

Revista Penal

Número 58

Sumario

Doctrina:

- ¿Genocidio en Gaza? Un análisis desde la perspectiva del Derecho Penal Internacional, por *Kai Ambos y Stefanie Bock* 5
- ¿Qué es lo que hace de un Código Penal un buen Código?, por *Jerónimo Bide* 14
- Normas penales y atribución de significado a través del proceso penal, por *Inês Fernandes Godinho* 39
- Aspectos jurídicos controvertidos de la incidencia de las tecnologías de la información en la comisión de delitos de blanqueo de capitales, por *Miguel Ángel Fernández-Salinero* 48
- Superinteligencia artificial penal: ¿Justicia algorítmica o Lombroso 4.0?, por *Juan Carlos Ferré Olivé* 64
- Derecho Penal y videojuegos: especial consideración de los *eSports*, por *David García Carmona* 81
- La ciberestafa amorosa: ¿engaño burdo u ofensa emocional más allá del patrimonio?, por *Elena Gutiérrez Pérez* 100
- Tefia y el derecho penal de autor: la criminalización de la identidad LGTBI en el franquismo, por *Florentino De Guzmán Plasencia* 121
- Perspectiva de género y razonamiento probatorio: hacia una teoría crítica de la prueba en los delitos sexuales, por *Manuel Pérez Mano* 134
- Hechos empresariales decididos por agentes de inteligencia artificial. Riesgo permitido y responsabilidad penal de las personas jurídicas, por *Sergio Pérez González* 150
- Localización permanente en centro penitenciario: ¿una pena de creación judicial y penitenciaria?, por *Cristina Rodríguez Yagüe* 178
- Dolo, alevosía y ensañamiento y su constatación en casos de anomalías o alteraciones psíquicas: ¿es posible imponer medidas de seguridad sin elementos subjetivos?, por *M^a del Valle Sierra López* 197

Sistemas penales comparados:

- El delito de tráfico de órganos (*Human organ trafficking*) 217

- Fe de Erratas 285

* Los primeros 31 números de la Revista Penal están recogidos en el repositorio institucional científico de la Universidad de Huelva Arias Montano: <https://hdl.handle.net/10272/11778>.

La Revista Penal puede consultarse íntegramente en <https://revistapenal.tirant.com/index.php/revista-penal/index>



UNIVERSIDAD
DE SALAMANCA



tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, y Pablo Olavide de Sevilla

Dirección

Juan Carlos Ferré Olivé. Universidad de Huelva
jcferrereolive@gmail.com

Directora de Edición

Carmen González Vaz. Universidad CUNEF, Madrid

Secretarios de redacción

Víctor Manuel Macías Caro. Universidad Pablo de Olavide
Miguel Bustos Rubio. Universidad Internacional de La Rioja

Comité Científico Internacional

Kai Ambos. Univ. Göttingen
Luis Arroyo Zapatero. Univ. Castilla-La Mancha
Ignacio Berdugo Gómez de la Torre. Univ. Salamanca
Gerhard Dannecker. Univ. Heidelberg
José Luis de la Cuesta Arzamendi. Univ. País Vasco
Norberto de la Mata Barranco. Univ. País Vasco
Jorge Figueiredo Dias. Univ. Coimbra
George P. Fletcher. Univ. Columbia
Luigi Foffani. Univ. Modena
Alfonso Galán Muñoz. Univ. Pablo de Olavide
Nicolás García Rivas. Univ. Castilla-La Mancha
Juan Luis Gómez Colomer. Univ. Jaume I^o
Carmen Gómez Rivero. Univ. Sevilla

José Luis González Cussac. Univ. Valencia
Carlos Martínez- Buján Pérez, Univ. A Coruña
Alessandro Melchionda. Univ. Trento
Victor Moreno Catena. Univ. Carlos III
Francisco Muñoz Conde. Univ. Pablo Olavide
Francesco Palazzo. Univ. Firenze
Teresa Pizarro Beleza. Univ. Lisboa
José Ramón Serrano Piedecabras. Univ. Castilla-La Mancha
Ulrich Sieber. Max Planck. Institut, Freiburg
Juan M. Terradillos Basoco. Univ. Cádiz
John Vervaele. Univ. Utrecht
Manuel Vidaurri Aréchiga. Univ. La Salle Bajío
Eugenio Raúl Zaffaroni. Univ. Buenos Aires

Consejo de Redacción

Miguel Ángel Núñez Paz y Susana Barón Quintero (Universidad de Huelva), Adán Nieto Martín, Eduardo Demetrio Crespo y Ana Cristina Rodríguez (Universidad de Castilla-La Mancha), Emilio Cortés Bechiarelli (Universidad de Extremadura), Fernando Navarro Cardoso y Carmen Salinero Alonso (Universidad de Las Palmas de Gran Canaria), Lorenzo Bujosa Badell, Eduardo Fabián Caparros, Nuria Matellanes Rodríguez, Ana Pérez Cepeda, Nieves Sanz Mulas y Nicolás Rodríguez García (Universidad de Salamanca), Paula Andrea Ramírez Barbosa (Universidad Externado, Colombia), Paula Bianchi (Universidad de Los Andes, Venezuela), Elena Núñez Castaño (Universidad de Sevilla), José León Alapont (Universidad de Valencia), Pablo Galain Palermo (Universidad Nacional Andrés Bello de Chile), Alexis Couto de Brito y William Terra de Oliveira (Univ. Mackenzie, San Pablo, Brasil).

Sistemas penales comparados

Christoph Hollmann (Alemania)
Luis Fernando Niño (Argentina)
Jakob Hajszan (Austria)
Alexis Couto de Brito y Jenifer Moraes (Brasil)
Fernanda Belén Aguirre Guerra (Chile)
Paula Andrea Ramírez Barbosa (Colombia)
Angie Andrea Arce Acuña (Costa Rica)
Antonio Rodríguez Molina (España)
Federica Raffone (Italia)

Manuel Vidaurri Aréchiga (México)
Sergio J. Cuarezma Terán (Nicaragua)
Campo Elías Muñoz Arango (Panamá)
Víctor Roberto Prado Saldarriaga (Perú)
Blanka Julita Stefańska (Polonia)
Volodymyr Hulkevych (Ucrania)
Pablo Galain Palermo (Uruguay)
Jesús Enrique Rincón Rincón (Venezuela)

<https://revistapenal.tirant.com/index.php/revista-penal/index>

© TIRANT LO BLANCH
EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELF.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email: tlb@tirant.com
<http://www.tirant.com>
Librería virtual: <http://www.tirant.es>
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
MAQUETA: Tink Factoría de Color

Si tiene alguna queja o sugerencia envíenos un mail a: atencioncliente@tirant.com. En caso de no ser atendida su sugerencia por favor lea en www.tirant.net/index.php/empresa/politicas-de-empresa nuestro procedimiento de quejas.

Responsabilidad Social Corporativa: <http://www.tirant.net/Docs/RSCtirant.pdf>



Derecho Penal y videojuegos: especial consideración de los *eSports*

David García Carmona

Revista Penal, n.º 58 - Julio 2026

Ficha Técnica

Autor: David García Carmona

Adscripción institucional: Doctor en Derecho. Coordinador técnico de TFE y prácticas de la Facultad de Derecho en la Universidad Internacional de La Rioja.

Investigador del grupo de investigación DDEPOR (UNIR)

ORCID: 0009-0009-3718-3027

DOI: <https://doi.org/10.36151/RP.58.06>

Title: Criminal Law and Video Games: Special Consideration of *eSports*

Sumario: I. INTRODUCCIÓN. II. OBJETIVOS Y METODOLOGÍA. III. BREVE CONTEXTO HISTÓRICO Y ACTUALIDAD DE LOS VIDEOJUEGOS Y DEPORTES ELECTRÓNICOS. IV. DELITOS INFORMÁTICOS EN LOS VIDEOJUEGOS. V. DELITOS DE DAÑOS INFORMÁTICOS EN LOS *ESPORTS*. VI. OTRAS MODALIDADES DELICTUALES EN LOS VIDEOJUEGOS Y EN LOS *ESPORTS*: ESPECIAL REFERENCIA A LA PROPIEDAD INTELECTUAL. VII. CONCLUSIONES. VII. REFERENCIAS BIBLIOGRÁFICAS.

Summary: I. INTRODUCTION II. OBJECTIVES AND METHODOLOGY III. BRIEF HISTORICAL CONTEXT AND CURRENT STATE OF VIDEO GAMES AND E-SPORTS. IV. COMPUTER CRIMES IN VIDEO GAMES. V. COMPUTER DAMAGE CRIMES IN *ESPORTS*. VI. OTHER CRIMINAL ACTIVITIES IN VIDEO GAMES AND *ESPORTS*: SPECIAL REFERENCE TO INTELLECTUAL PROPERTY. VII. CONCLUSIONS. VIII. BIBLIOGRAPHICAL REFERENCES.

Resumen: El presente texto interrelaciona el Derecho Penal con el sector de los videojuegos, haciendo especiales consideraciones sobre los deportes electrónicos. Se parte de una necesaria contextualización de los videojuegos y de los deportes electrónicos para, a partir de ella, ahondar en las conductas criminales que pueden acontecer en el referido sector, incidiendo especialmente en los delitos de daños informáticos, delitos contra la propiedad intelectual abordando además de una forma sucinta otras potenciales actividades ilícitas a partir de un razonamiento hipotético deductivo.

Palabras clave: Derecho Penal, delitos informáticos, cibercriminalidad, videojuegos, *eSports*.

Abstract: This text examines the intersection between Criminal Law and the video game sector, with particular attention to electronic sports. It begins with a necessary contextualization of video games and esports, and from this foundation, it delves into the criminal behaviors that may arise within the sector, focusing especially on computer-related offenses, intellectual property crimes, and doping offenses, while also briefly addressing other potential illicit activities through a deductivehypothetical reasoning approach

Key words: Criminal Law, computer crimes, cybercrime, doping, video games, *eSports*

Observaciones: este trabajo se desarrolla dentro de una de las principales líneas de investigación del Grupo de Investigación en Derecho Deportivo (DDEPOR) en UNIR.

Rec.: 12-12-2025 **Fav.:** 13-05-2026

I. INTRODUCCIÓN

El avance de las nuevas tecnologías, que combina no solo el uso de los componentes físicos y operativos de un ordenador (*hardware*), sino también la explotación de datos y bases de datos gestionadas mediante los componentes lógicos (*software*) necesarios para ejecutar determinadas tareas, ha provocado una auténtica transformación en el funcionamiento de las sociedades modernas, especialmente en las más desarrolladas. Esta revolución no se limita a actividades complejas, sino que alcanza también a las más habituales y cotidianas. Los datos informáticos, los documentos electrónicos y los programas constituyen un soporte intangible que sustenta buena parte de la actividad comercial, científica, sanitaria y administrativa, así como aspectos relevantes de los derechos individuales, como la intimidad, las comunicaciones, la propiedad, las creencias y la ideología. En un mundo interconectado, prácticamente cualquier dimensión de la vida personal o colectiva depende de los datos digitales, sus colecciones y los programas que los gestionan. Esta evolución y creciente importancia ha dado lugar a la aparición de nuevos fenómenos delictivos, derivados del uso indebido de la tecnología, que se manifiestan, entre otras formas, mediante conductas dirigidas a impedir que el titular del recurso digital pueda utilizarlo, ocasionándole un perjuicio en alguno de sus intereses¹.

La cada vez mayor incidencia de las manifestaciones criminales cometidas directamente contra los sistemas informáticos y a través de estos, para atacar contra diversos bienes jurídicos, como el honor y la intimidad, e incluso contra la propia seguridad del Estado, ha fomentado una percepción social de peligrosidad, de estas actuaciones, agravada por las evidentes dificultades para su persecución y descubrimiento, así como para la identificación de las personas responsables de estos comportamientos.

Pese a ello, se adelanta que el Código Penal, en adelante CP, no contiene, como tal, ni un delito informático². En este sentido, se está de acuerdo con lo afirmado por Romeo Casabona³, y recuerda Hernández Díaz⁴, y es que no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que la única nota común es su vinculación de alguna manera con los ordenadores.

Así, la expresión “delitos informáticos” surgió para describir una modalidad de criminalidad emergente asociada al desarrollo de los primeros sistemas informáticos, en la que dichos sistemas podían operar bien como instrumento para la comisión de la infracción, bien como objeto material directo de la conducta delictiva. Con el paso del tiempo, esta categoría descriptiva se ha ido ampliando hasta abarcar conductas heterogéneas, cuya nota común no reside en su estructura típica, sino en su vinculación funcional con entornos digitales y redes de comunicación, lo que ha llevado a emplear de forma creciente el concepto de cibercrimen para aludir a este conjunto de fenómenos.

Todos estos comportamientos pueden encuadrarse, en sentido amplio, en el concepto de cibercriminalidad, entendido como el conjunto de conductas delictivas que se desarrollan en un entorno caracterizado por el uso intensivo de tecnologías de la información y la comunicación y por dinámicas de actuación sustancialmente distintas de las propias del ámbito físico tradicional. Esta especificidad del espacio digital no implica la aparición de un fenómeno penal autónomo, pero sí condiciona las formas de comisión, los medios empleados y los efectos de las conductas, lo que exige un análisis jurídicopenal atento a las particularidades del entorno en el que se producen los hechos y a su correcta subsunción en los tipos penales existentes, sin que ello suponga, por sí mismo, una revisión global del sistema ni una reformulación de sus fines preventivos⁵.

En este sentido, y siguiendo la concepción propuesta por Miró Llinares, el cibercrimen puede definirse como “cualquier comportamiento delictivo realizado en el ciberespacio”, entendido este como el ámbito virtual de interacción y comunicación personal definido por el uso de las tecnologías de la información y la comunicación. Desde esta perspectiva, se incluyen tanto conductas cuyo contenido ilícito resulta relativamente novedoso por hallarse vinculado a intereses o bienes específicos del entorno digital, como comportamientos tradicionalmente delictivos que, sin ver alterada su estructura esencial, se llevan a cabo a través de Internet u otros medios telemáticos. Este planteamiento permite abordar el fenómeno desde categorías penales ya conocidas, sin necesidad de articular un Derecho penal autónomo o diferenciado para el ámbito digital, y proporciona un marco conceptual adecuado para el análisis

1 Sentencia del Tribunal Supremo de 7 de febrero de 2022. FD 5º STS 528/2022 - ECLI:ES:TS:2022:528.

2 PÉREZ ARIAS, J. (2021). “Cibercriminalidad: hacia la nueva realidad —virtual— del derecho penal”. *Revista Internacional de Doctrina y Jurisprudencia*, vol. 26. p. 176.

3 ROMEO CASABONA, C.M. (1988). *Poder informático y seguridad jurídica. la función tutelar del derecho penal ante las nuevas tecnologías de la información*. Madrid, pp. 42 y ss.

4 HERNÁNDEZ DÍAZ, L. (2009). “El delito informático”. *EGUZKILORE*, núm. 23, San Sebastián, diciembre, p. 233.

5 Cfr. MIRÓ LLINARES, F. (2011). “La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen”. *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13, p. 3

sis posterior de aquellas conductas que, por sus características, pueden manifestarse en el ámbito específico de los videojuegos y de los deportes electrónicos⁶.

Merece la pena traer a colación en este mismo sentido sobre el incremento de la preocupación sobre estas modalidades delictivas que, en el año 2017, la Secretaría de Estado de Seguridad, órgano dependiente del Ministerio del Interior, elaboró un Estudio sobre la Cibercriminalidad en España y, en él, señala que “la ciberdelincuencia, como fenómeno que va parejo al uso de las nuevas tecnologías, ha experimentado un crecimiento durante los últimos años, como consecuencia de un mayor uso por parte de la sociedad de todas las nuevas formas de conectividad tecnológica”⁷.

II. JUSTIFICACIÓN, OBJETIVOS Y METODOLOGÍA

La elección del objeto de estudio y de las tipologías delictivas analizadas en el presente trabajo responde a una deliberada toma de posición teórica y metodológica. Lejos de pretender una exposición exhaustiva de todas las conductas punibles susceptibles de manifestarse en el entorno de los videojuegos y de los deportes electrónicos, el análisis se concentra en aquellas infracciones que presentan una vinculación estructural directa con las características técnicas, económicas y organizativas del sector, y que, al mismo tiempo, plantean problemas dogmáticos relevantes desde la perspectiva del Derecho Penal vigente.

En este sentido, los delitos informáticos y, en particular, los delitos de daños y sabotaje informático han sido seleccionados como eje central del estudio por cuanto inciden directamente sobre los elementos constitutivos del ecosistema digital como los sistemas informáticos, programas, datos y servicios cuya disponibilidad, integridad y funcionamiento resultan esenciales tanto para el entretenimiento digital como para la competición profesionalizada. A diferencia de otros ilícitos que pueden producirse de manera contingente en el ciberespacio, estas conductas no constituyen meras traslaciones tecnológicas de criminalidades tradicionales, sino que explotan de forma específica las singularidades del medio y generan riesgos inéditos en términos de afectación patrimonial, funcional y social.

Junto a los delitos de daños informáticos, la atención prestada a los delitos contra la propiedad intelectual responde a la constatación de que los videojuegos constituyen obras de autoría compleja y que la piratería digital, lejos de ser un fenómeno marginal, se configura como una práctica de elevada lesividad económica y

sistemática. La vulneración masiva de derechos de propiedad intelectual en este ámbito no solo compromete intereses económicos privados, sino que incide directamente en la sostenibilidad de una industria cultural de primer orden, lo que justifica su examen diferenciado desde una perspectiva penal material.

Por el contrario, se ha optado conscientemente por no abordar con igual profundidad otras modalidades delictivas como determinados delitos contra el honor, estafas genéricas, injurias o amenazas que, aun pudiendo producirse en el contexto analizado, no presentan un anclaje estructural específico en la lógica propia de los videojuegos y los *eSports*. Su inclusión habría diluido el objetivo del trabajo y desplazado el foco desde aquellas infracciones que ponen en cuestión los límites dogmáticos de la tipicidad penal informática hacia un catálogo heterogéneo de conductas cuya relevancia no depende del sector estudiado, sino del medio digital en un sentido amplio.

El objetivo principal del trabajo consiste, así, en examinar la adecuación del marco penal español para abordar las manifestaciones más relevantes de criminalidad informática en el ámbito de los videojuegos y de los deportes electrónicos, identificando los principales problemas interpretativos que plantean los tipos aplicables, en especial en lo relativo a la determinación del bien jurídico protegido, la delimitación de la gravedad penalmente relevante y la correcta subsunción de las conductas en preceptos diseñados originalmente para entornos distintos. De forma complementaria, se persigue evidenciar las tensiones existentes entre el principio de intervención mínima y la necesidad de una tutela penal eficaz frente a fenómenos delictivos que producen daños de considerable entidad económica y social.

Desde el punto de vista metodológico, el trabajo adopta una aproximación dogmáticojurídica, centrada en el análisis sistemático de los preceptos relevantes del Código Penal español, con atención a su evolución legislativa, a la interpretación doctrinal dominante y a la jurisprudencia más significativa. Este análisis se complementa con referencias a normativa europea y a pronunciamientos judiciales extranjeros cuando resultan útiles para ilustrar supuestos de hecho aún poco desarrollados en la práctica judicial española. No se pretende realizar un estudio empírico ni criminológico en sentido estricto, sino ofrecer una reconstrucción penal técnicamente rigurosa, capaz de orientar la subsunción y de poner de relieve los déficits y potencialidades del sistema penal ante un fenómeno en rápida expansión.

Asimismo, el enfoque metodológico incorpora una dimensión contextual, en la medida en que las conduc-

6 MIRÓ LLINARES, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, p. 42.

7 AAVV. *Estudio sobre la Criminalidad en España*. Ministerio del Interior, Madrid, 2017, p. 3.

tas analizadas se sitúan en escenarios reales o verosímiles del sector de los videojuegos y los eSports. Esta contextualización no persigue una finalidad descriptiva autónoma, sino que cumple una función instrumental: permitir una mejor comprensión de la dinámica comitiva y del impacto funcional de los ilícitos, evitando interpretaciones excesivamente abstractas o descontextualizadas del tipo penal. En definitiva, el trabajo se inscribe en una concepción del Derecho penal como última ratio, atento a los cambios tecnológicos y sociales, pero firme en la preservación de sus principios estructurales de legalidad, culpabilidad y proporcionalidad.

III. VIDEOJUEGOS Y DEPORTES ELECTRÓNICOS: BREVE CONTEXTO Y SITUACIÓN ACTUAL

Se deja constancia al inicio del presente apartado de que no es su objetivo hacer un estudio detallado y pormenorizado de la evolución histórica del sector de los videojuegos y de la industria de los deportes electrónicos hasta llegar a la actualidad⁸, sino que se pretende evidenciar, de forma clara y sintetizada, su existencia y registro desde hace medio siglo y de su gran crecimiento y auge durante tales décadas hasta llegar a adquirir en la actualidad una notoria repercusión tanto social como económica.

Pues bien, si se avanza hacia el objeto de estudio del presente texto, es decir, los videojuegos y los deportes electrónicos⁹, ha de destacarse que son medios de entretenimiento digital que, como se indicaba de forma previa, han experimentado un gran crecimiento en los últimos años en la sociedad global, si bien es cierto que se llevan consumiendo como elemento de ocio y de diversión desde hace décadas.

En este sentido e incidiendo así, de forma breve y sucinta en la historia de la industria de los videojuegos

y de su ulterior factor competitivo, destaca, tanto como referente como por ser el punto de partida, en la década de los años setenta, el videojuego *SpaceWar*¹⁰.

Como se ha indicado previamente, no solo los videojuegos tienen sus orígenes hace décadas¹¹, sino que también es así para los eSports¹² destacando como hitos relevantes la primera competición en 1972 promovida por la Universidad de Stanford, las famosas “Olimpiadas Intergalácticas de Guerra espacial” en las que diversos jugadores compitieron entre sí al videojuego *Spacewar*¹³ o los “Campeonatos del Mundo Nintendo” de Estados Unidos (EE.UU en adelante) en la década de los 90¹⁴.

Tras destacar alguno de los hitos más relevantes de los videojuegos y de los deportes electrónicos, en cada una de las décadas del siglo pasado partiendo desde su concepción y su acogimiento en Europa en la primera década de los años 2000, para apreciar, de forma genérica, la magnitud y el impacto que la industria del videojuego proyecta sobre la sociedad contemporánea, resulta ilustrativo acudir a los datos publicados por la consultora Newzoo en 2023¹⁵, entidad de reconocido prestigio tanto en el ámbito del videojuego como en el ecosistema competitivo digital. De acuerdo con dicha fuente, si se consideran en conjunto las diversas plataformas existentes, esto es, los distintos medios de acceso al contenido video lúdico, desde teléfonos inteligentes hasta ordenadores y consolas, casi la mitad de la población mundial participa actualmente en actividades relacionadas con los videojuegos.

Desde una perspectiva más concreta, y atendiendo a la realidad de nuestro país, la referida consultora, Newzoo, señala que España alcanzó en 2020 la décima posición mundial por volumen de ingresos en el sector, con una facturación de 2.656 millones de dólares, si bien en

8 Este objetivo ha sido ya evidenciado en otras contribuciones del propio autor que suscribe este texto, de las que se deja reflejo y evidencia en ulteriores notas al pie de página.

9 La distinción entre videojuegos y deportes electrónicos se explica con detalle en García Carmona, D. (2026). *Riesgos delictivos en el entorno de los deportes electrónicos*. Tesis Doctoral. Universidad de La Rioja., pero se reproduce, por considerarse acertada, la máxima de que todos los eSports son videojuegos, pero no todos los videojuegos son eSports a la que se alude en el apartado V del presente texto.

10 Videojuego en el que dos jugadores, cada uno manejando una pequeña nave espacial, deben encontrar la manera de destruir la nave de su oponente, gestionando su armamento y combustible.

11 Para una información más detallada sobre el contexto histórico de los eSports al respecto, véase GARCÍA CARMONA, D. (2025). “eSports” o deportes electrónicos: un breve recorrido en la normativa nacional e internacional”. En MILLÁN GARRIDO, A. y RODRÍGUEZ TEN, J. (coords.). *La dimensión internacional del deporte*. Reus. Madrid, pp. 64 y ss; y GARCÍA CARMONA, D., “eSports: Origen, Presente y Futuro”. *Revista Electrónica de Derecho de La Universidad de La Rioja (REDUR)*, núm. 19, 2021, pp. 109-117.

12 Cabe precisar en este momento que, si bien podría englobarse todo dentro del concepto de eSports, no son exactamente iguales las concepciones de eSports del pasado y el concepto que tenemos presente hoy en día, ya que, hace décadas, las competiciones de videojuegos no presentaban las notas de profesionalidad, estructura y competición que las caracteriza en el sector actual.

13 Información obtenida en: <https://www.ispo.com/es/negocio-del-deporte/historia-de-los-esports-como-empezotodo#:~:text=Pe-ro%20el%2019%20de%20octubre,entre%20s%C3%AD%20en%20%22%C2%A1Spacewar!> Última consulta: 24/01/2025.

14 Información obtenida en: <https://www.marca.com/videojuegos/otros-juegos/2020/11/03/5fa11edc46163fa7508b462d.html>. Última consulta: 25/01/2025.

15 Newzoo. Global Games Market Report. 2023.

la actualidad ya no figura entre los diez primeros países en esta clasificación¹⁶.

En lo que respecta específicamente al ámbito de los deportes electrónicos, la posición de España muestra igualmente rasgos distintivos de gran relevancia. El país constituye el único Estado europeo en el que las tres principales operadoras de telecomunicaciones, en concreto, Orange, Vodafone y Movistar, han decidido integrarse activamente en la industria, lo que evidencia un notable grado de consolidación del sector. España alberga, además, la mayor competición nacional de Europa, la LVP, y se ha configurado como sede estable de importantes franquicias internacionales, entre las que destacan ESL y DreamHack. El territorio español acoge igualmente eventos de gran formato y notable repercusión, tanto periódicos, como el Barcelona Games World, Madrid Gaming Experience, Tenerife LAN Party o Euskal Encounter, como extraordinarios, incluyendo celebraciones vinculadas a la League of Legends Championship Series (LCS) o a los All Star de carácter mundial. A ello se suma la incorporación de marcas comerciales de primer nivel, entre ellas Bimbo y El Corte Inglés, que han optado por patrocinar equipos o competiciones nacionales, lo cual refuerza la relevancia económica y social de este ecosistema¹⁷.

En relación con el sector de los deportes electrónicos, resulta imprescindible subrayar que en los últimos años ha experimentado un crecimiento económico particularmente acusado, reflejado en ingresos que superan los mil millones de dólares a escala global. En el caso de España, las estimaciones apuntan a la existencia de tres millones de seguidores, en contraste con los más de quinientos millones registrados mundialmente en 2022, según los datos publicados por Newzoo¹⁸. Dicha consultora sitúa, además, la facturación del sector español en torno a los 27 millones de euros.

El informe elaborado por la misma firma para el primer trimestre de 2021 proyectaba, asimismo, que los ingresos globales del sector alcanzarían ese año 1.084 millones de dólares, lo que implicaba un incremento del 14 % con respecto a los valores correspondientes a

2020¹⁹. En términos de audiencia, se estimaba un total de 728 millones de espectadores de competiciones en directo, cifra que supondría a su vez un incremento del 10 % respecto del número de consumidores de contenidos de deportes electrónicos registrado en 2020²⁰.

Entre los hitos más recientes, destaca especialmente la celebración, en agosto de 2024 en Riad, de la Esports World Cup (EWC), organizada por la Esports World Cup Foundation (EWCF), entidad de naturaleza no lucrativa²¹. Este evento congregó a quinientos millones de espectadores, que consumieron más de doscientos cincuenta millones de horas de contenido, configurándose, sin margen de duda, como el torneo más visto del año 2024. La repercusión económica del evento fue igualmente notable: la competición distribuyó más de sesenta millones de dólares en premios, lo que la convirtió en la mayor bolsa económica de la historia de los eSports, al tiempo que la ciudad experimentó un aumento del 30 % en la actividad turística y recibió más de dos millones de visitantes²².

En lo que respecta a la proyección futura del sector, cabe finalmente destacar que en 2027 se celebrará en Riad la primera edición de los Juegos Olímpicos de eSports, decisión adoptada en la 142.ª sesión del Comité Olímpico Internacional (COI), celebrada en julio de 2024, en la que se acordó formalmente la creación de esta nueva modalidad olímpica²³.

La concurrencia de todos estos factores, unida al vertiginoso desarrollo de las infraestructuras de conectividad y al avance tecnológico en ámbitos como la capacidad de procesamiento de datos, los algoritmos, la potencia gráfica o la implementación del 5G, ha impulsado de manera decisiva la expansión de los deportes electrónicos. No obstante, esta misma evolución, acompañada del elevado volumen económico que movilizan tanto sus competiciones como su organización, ha provocado que el sector se convierta simultáneamente en un foco creciente de interés para la delincuencia, utilizándose en ocasiones como medio o canal para la comisión de conductas delictivas.

16 Información obtenida en: <https://newzoo.com/resources/rankings/top-10-countries-by-game-revenues>. Última consulta: 27/01/2025.

17 *Guía Legal sobre los e-Sports. Presente y futuro de la regulación de los e-Sports en España*, edit. ONTIER -Liga Profesional de Videojuegos, edición 2018, p. 12.

18 NEWZOO. *Global Esports & Live Streaming Market Report*. 2022, p. 31.

19 Información obtenida en: <https://newzoo.com/resources/trend-reports/newzoos-global-esports-live-streaming-market-report-2021-free-version>. Última consulta: 03/03/2025.

20 WEZENBEEK, R., "Reportaje: el nuevo paradigma del sector audiovisual". *Bit. La revista profesional sobre tecnología y transformación digital*, núm. 223. COIT y AEIT, 2022, p. 10.

21 Cfr. GARCÍA CARMONA, D. (2025). *op. cit.*, p. 79.

22 Información obtenida en: <https://esportsbureau.com/la-esports-world-cup-atrae-a-mas-de-500m-de-telespectadores-y-team-falcons-se-corona-como-primer-campeon-de-clubes/>. Última consulta: 08/03/2025.

23 Información obtenida en: <https://www.coe.es/noticias/detalle-noticia/NEW-413d0426-e546-4ea9-9d41-1f84ca80a242/los-primeros-juegos-olimpicos-de-esports-se-celebraran-en-riad-en-2027/>. Última consulta: 17/02/2025.

IV. DELITOS INFORMÁTICOS EN LOS VIDEOJUEGOS

Una vez evidenciada la realidad axiomática que orbita sobre los videojuegos y los deportes electrónicos, es momento de analizar ciertas acciones que pueden darse en estos sectores y subsumirlas en el Derecho Penal.

De forma previa al análisis de algunas de las diversas tipologías delictuales referidas, es necesario recordar que, en el presente texto pese que ya se ha destacado en el apartado correspondiente sobre los objetivos y metodología, se analizan aquellas conductas delictuales que con cierta base probabilística pueden acontecer, por sus características tan particulares y su vinculación estructural directa con las características técnicas, económicas y organizativas del sector tanto de los videojuegos como de los deportes electrónicos y que, al mismo tiempo, plantean problemas dogmáticos relevantes desde la perspectiva del Derecho Penal vigente.

Asimismo, debe precisarse que el presente trabajo no pretende ofrecer un catálogo exhaustivo o *numerus clausus* de las posibles actividades ilícitas que pueden manifestarse en el ámbito de los videojuegos y de los deportes electrónicos. Tampoco se aborda un análisis detallado de la teoría del delito aplicable a cada una de las conductas examinadas, ámbito que ha sido ya tratado con notable rigor y profundidad por una amplia doctrina especializada. La finalidad del estudio se orienta, más bien, a profundizar en la descripción y contextualización de determinadas conductas especialmente significativas, analizando los escenarios en los que se han producido o pueden razonablemente producirse y realizando, a partir de ellos, un ejercicio de subsunción conforme a las disposiciones del Derecho penal español, aun cuando algunos de los supuestos considerados tengan su origen en otros ordenamientos jurídicos.

Se reitera que este conjunto heterogéneo de conductas integra lo que hoy se entiende por cibercriminalidad y resulta evidente que, en el contexto social contemporáneo, dicho concepto abarca un amplio espectro de actividades ilícitas relacionadas con el acceso, la obtención, la transmisión y la manipulación de datos e información mediante redes telemáticas, las cuales

constituyen el entorno operativo y comisivo propio de esta forma de delincuencia²⁴.

Como se expresaba con anterioridad en el presente texto, en nuestro ordenamiento jurídico, en concreto, en el CP, no existe dentro de ningún título o capítulo, una categoría específica de “delitos informáticos”, si bien es cierto que estas tipologías delictuales se recogen en diversos preceptos del citado cuerpo normativo.

Entre otras tipologías delictuales, se considera apropiado por su posible perpetración en el sector de los videojuegos, destacar las siguientes:

- Delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el artículo (en adelante art.) 264 y concordantes del CP.
- Delitos de descubrimiento y revelación de secretos del art. 197 CP cometidos a través de las nuevas tecnologías o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.
- Delitos contra la propiedad intelectual, del art. 270 CP.
- Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el art. 286 CP²⁵.

Aclarado lo anterior, debe entenderse por sistema informático: “todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento”²⁶ y por dato informático²⁷: “toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función”²⁸.

En el contexto de los videojuegos, algunos de los delitos informáticos y/o modalidades de comisión más comunes son los siguientes:

- Acceso no autorizado a sistemas informáticos: este delito consiste en acceder a un sistema in-

24 ROMEO CASABONA, C. (2006). *De los delitos informáticos al cibercrimen. El cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales*, Comares, Granada, p. 9.

25 Estos son algunos de los muchos delitos que se pueden cometer por medio electrónicos y que recoge y expone de manera sucinta la doctrina de la Fiscalía General del Estado en la Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías.

26 Art. 2.a de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

27 En profundidad, sobre estos conceptos y su aplicación a los delitos informáticos, véase DE LA MATA BARRANCO, N.J. y HERNÁNDEZ DÍAZ, L. (2009). “El delito de daños informáticos: una tipificación defectuosa”. *Estudios Penales y Criminológicos*, núm. 29, p. 321.

28 Art. 2.b de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

formático sin autorización. En los videojuegos este delito puede consistir en *hackear* un servidor para obtener información confidencial, como datos de usuarios o contraseñas.

Esta tipología delictiva, se introdujo en 2010, con la Ley Orgánica 5/2010, de 22 de junio, en cuya Exposición de Motivos, se justificaba la incorporación de esta figura como un ajuste a la ‘Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información’.

En este sentido, se decidió estructurar las conductas punibles del tipo en dos apartados diferenciados, dada la diversidad de los bienes jurídicos protegidos. El primero engloba los daños, incluyendo acciones destinadas a dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como a obstaculizar o interrumpir el funcionamiento de un sistema informático. El segundo apartado se refiere al descubrimiento y revelación de secretos, abarcando el acceso no autorizado que vulnera las medidas de seguridad sobre datos o programas contenidos en un sistema o en una parte del mismo.

No obstante, pese a lo anterior, parece haber cierto consenso en entender que, con carácter general, el bien jurídico que se protege en este ilícito, es el mismo bien jurídico que cuando se sancionan conductas de daños sobre objetos corpóreos, materiales y físicos, es decir, la propiedad ajena y el patrimonio²⁹.

Resulta asimismo relevante destacar que parte de la doctrina ha defendido una concepción distinta del bien jurídico protegido en esta categoría de delitos informáticos. Así, autores como Hernández Díaz consideran que la tutela penal no se agota en la protección fragmentaria de bienes jurídicos individuales, sino que se proyecta sobre un bien jurídico colectivo y de carácter indisponible, identificado con la seguridad informática. En este sentido, se sostiene que se “trata de un bien cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual puestos en peligro con tales conductas atentatorias contra la seguridad de las redes y sistemas informáticos, pero no siempre efectivamente dañados y que no encuentra suficiente protección mediante la salvaguarda en exclusiva de bienes jurídicos de naturaleza individual”³⁰. Desde esta perspectiva, la intervención penal se justifica no solo

por el daño efectivamente producido, sino también por la necesidad de garantizar la fiabilidad, estabilidad y seguridad global de los sistemas y redes informáticas como presupuesto estructural del ejercicio de múltiples derechos individuales

Es claro que, pese a interpretaciones, la configuración normativa del 264.1 adquiere una importancia decisiva, pues no resulta suficiente cualquier afectación al bien jurídico, sino que dicha lesión ha de rebasar un umbral mínimo de relevancia. De este modo, y para evitar que el tipo penal pierda contenido, la noción de ‘gravedad’ no puede derivarse ni del modo de ejecución ni de los efectos externos de la conducta, sino que ha de venir definida por las características intrínsecas de la información dañada³¹.

Del examen del tipo penal y en consonancia con lo anterior, se desprende que los daños informáticos resultan atípicos cuando el resultado en su expresión más elemental no reviste gravedad. Ahora bien, este es un concepto de naturaleza normativa que no puede determinarse mediante un parámetro exclusivamente cuantitativo, como sería considerar irrelevantes aquellos supuestos en los que el perjuicio no supera los 400 euros. La gravedad debe apreciarse atendiendo al menoscabo funcional que compromete el funcionamiento del sistema. Su constatación es patente, desde luego, cuando la plena operatividad del sistema no puede restablecerse. Asimismo, y siguiendo la orientación de la Circular 3/2017 de la Fiscalía General del Estado, puede estimarse que concurre la gravedad típica cuando la restitución del sistema requiere un esfuerzo técnico y económico especialmente elevado³².

No obstante, conviene recordar que el manejo de la información presenta una notable complejidad y exige atender a las particularidades del objeto material del delito para valorar la gravedad prevista en el artículo 264.1 CP de forma realista, coherente y evitando apreciaciones arbitrarias. En el ámbito del ciberespacio, los problemas dogmáticos rara vez admiten respuestas simples.

Así pues, la exigencia de gravedad impregna tanto la configuración del tipo básico como la de sus modalidades agravadas. No basta con que el resultado sea grave: también la conducta de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los datos o el sis-

29 ORTS BERENGUER, E. y ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, pp. 81 y ss.

30 HERNÁNDEZ DÍAZ, L. (2009). “El delito informático”, op. cit. p. 237. Cfr. En este sentido ARRASCO ANDRINO, M.M. (2009). “El acceso ilícito a un sistema informático”. En ÁLVAREZ GARCÍA, F.J., MANJÓN-CABEZA OLMEDA, A. y VENTURA PÜSCHEL, A. (coords.). *La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*. Tirant lo Blanch. Valencia, pp. 341-365.

31 REQUEJO-PASSONI, W. (2024). “El dilema de las copias de seguridad en el delito de sabotaje contra datos informáticos en el derecho penal español”. *Revista de Internet, Derecho y Política*, núm. 41, p. 8.

32 Sentencia del Tribunal Supremo de 20 de mayo de 2020. FD 4º de la STS 1520/2020 - ECLI:ES:TS:2020:1520.

tema debe revestir esa cualidad. Ahora bien, no resulta sencillo graduar la gravedad de la acción sin atender al resultado que, conforme a la voluntad del legislador, igualmente ha de ser grave. Estamos, por tanto, ante una gravedad de carácter concatenado y acumulativo, cuya afirmación no siempre será evidente. Una intervención mínima, como la simple ejecución de determinados comandos o teclas, puede generar daños informáticos de gran entidad que lleguen incluso a inutilizar el sistema. En tales supuestos, la escasa entidad de la acción contrasta con la severidad del resultado, lo que plantea serias dudas respecto a su adecuación típica.

En cuanto al objeto material lo constituyen los datos, ficheros, documentos o programas de *software*, todos ellos elementos lógicos de un sistema informático necesarios para posibilitar o facilitar el desarrollo de determinadas tareas. Se trata de un objeto de naturaleza inmaterial que puede definirse como un flujo electromagnético³³. Si bien es cierto que parte de la doctrina considera que el sabotaje informático a los datos ha de valorarse en cuanto a su valor funcional dentro del sistema en su conjunto o para la información que representa³⁴.

En cuanto a las posibles conductas típicas del ilícito, se reproducen en el tipo aquellas que se recogen en la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, en la que se expresa que: “Se mantienen las de borrar, dañar, deteriorar, alterar, suprimir y hacer inaccesibles, ya contempladas en la legislación precedente, siguiendo también en este aspecto la relación de comportamientos que recogen la Directiva 2013/40/UE en su art. 5, relativo a la interferencia ilegal en los datos, y la Decisión Marco 2005/22/JAI en su art. 4. De esta forma el Legislador pretende abarcar todas las posibles conductas susceptibles de afectar a los elementos informáticos, tanto aquellas que impliquen su destrucción, bien sea total o parcial, como aquellas otras que comporten una modificación —alteración— de los mismos que igual podría producirse por eliminación, supresión

o borrado parcial del elemento afectado como por la incorporación de nuevos datos que impliquen la variación del alcance o contenido inicial de aquellos”.

El tipo sanciona a quien, por cualquier procedimiento, sin autorización y de forma significativa, elimine, dañe, deteriore, modifique, suprima o vuelva inaccesibles datos, programas informáticos o documentos electrónicos. Mediante esta amplia gama verbal, el legislador pretende abarcar tanto las actuaciones que conllevan la destrucción total o parcial del objeto protegido, como aquellas que simplemente alteran sus componentes informáticos, ya sea mediante su eliminación, supresión o borrado parcial, o mediante la introducción de información nueva que modifique el contenido o alcance original de esos elementos³⁵.

De esto cabe deducir que se trata de un delito de medios que abarca desde el borrado manual a la utilización de virus actuando siempre sin autorización³⁶. No obstante, no toda la doctrina coincide en esta apreciación puesto que algún autor lo considera como un delito de resultado³⁷.

En cuanto a lo que al sujeto activo del ilícito respecta se está de acuerdo en que cobra especial relevancia la ajenedad del ataque³⁸ en cuestión puesto que, si fuese el mismo propietario el que produce, por ejemplo, la destrucción de archivos o datos informáticos en general no cabría analizar conducta típica alguna.

Una vez analizados levemente los elementos del tipo, cabe exponer una casuística real acontecida hace unos años, aunque fuera de España, el departamento de justicia del Distrito sur de California condenó a un joven a 27 meses de prisión por *hackear* un servidor de videojuegos (afectó a los videojuegos *Dota* y *League Of Legends*) para obtener información confidencial de los usuarios. En concreto, el ataque fue de Denegación de Servicio Distribuido, es decir, con ese ataque negó el servicio de accesos en línea a terceros sin que pudieran acceder a sus cuentas en las que se contiene información delicada y, por supuesto, de carácter personal³⁹.

Si se analiza este supuesto con nuestra normativa penal, se puede pensar que la subsunción de esta tendría cabida en el tipo recogido en el art. 264 *bis* del CP,

33 ANDRÉS DOMÍNGUEZ, A. C. (2015). “Comentario previo a los artículos 264, 264 bis, 264 ter y 264 quater”. En GÓMEZ TOMILLO, M. (dir.), *Comentarios prácticos al Código penal, Tomo III, Delitos contra el Patrimonio y socioeconómicos*, Aranzadi, Pamplona, p. 350.

34 MORALES GARCÍA, O. (2011). “Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas” en QUINTERO OLIVARES, G. (dir.), *La Reforma penal de 2010: Análisis y comentarios*, Aranzadi-Thomson, Madrid, p. 189.

35 Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, p. 21.

36 GORJÓN BARRANCO, M.C. (2021). “Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del código penal. especial referencia a su comisión con finalidad terrorista”. *Revista de Derecho Penal y Criminología*, 3.ª Época, núm. 25, p. 103.

37 GALÁN MUÑOZ, A. (2019). *Daños informáticos*. FUOC. Barcelona, p. 10.

38 ANDRÉS DOMÍNGUEZ, A. C. (2015), *op. cit.* pp. 351 y ss.

39 Información disponible en: <https://www.fayerwayer.com/2019/07/condenan-hacker-videojuegos-27-meses-prision/>. Última consulta: 22/01/2025.

es decir, como delito de sabotaje informático⁴⁰, puesto que se interrumpió, de forma grave y sin ningún tipo de autorización, el funcionamiento de un videojuego. No obstante, al entender que los videojuegos no se consideran sistemas informáticos sino programas o aplicaciones informáticas debido a que se “programan”⁴¹ en algún lenguaje para que se pueda utilizar en un sistema informático como una aplicación, este supuesto de hecho tendría cabida en el art. 264 CP, es decir, en el tipo básico ya que altera y hace inaccesibles programas y datos informáticos como consecuencia de una acción no consentida y que afecta gravemente a miles de personas.

No obstante, en nuestra jurisprudencia hay un caso ciertamente significativo sobre un supuesto de denegación de servicios distribuidos, en concreto, el caso en el que se enjuició a *Anonymous*. En este procedimiento varias personas fueron acusadas de llevar a cabo un ataque informático, Denegación de Servicios Distribuido (DDos) a la web de la Junta Electoral Central y la del Congreso en mayo de 2011, que afectó de forma importante al normal funcionamiento del correo electrónico, obstaculizando de tal modo los trámites previos y necesarios al proceso electoral y ocasionando igualmente el bloqueo de la página web de la Junta electoral central. Así como de perpetrar otro ataque DDoS con la llamada operación “V de Votaciones” contra las páginas web del Partido Popular (PP), del Partido Socialista Obrero Español (PSOE) y de Convergencia i Unió (CIU)⁴². El Ministerio Fiscal acusó por el delito del art. 264.2 del CP, aunque finalmente los acusados quedaron absueltos por la falta de pruebas⁴³.

Otro ejemplo paradigmático de esta modalidad delictiva de acceso no autorizado a un sistema informático, avanzando respecto a las casuísticas anteriores sobre DDoS, lo constituyó el ataque dirigido contra la plata-

forma PlayStation en 2011, incidente que comprometió la información personal de más de setenta millones de usuarios a escala global y que se erigió en uno de los episodios más significativos de vulneración de la seguridad en la industria del videojuego⁴⁴.

· Distribución de *malware*: esta modalidad delictual consiste en distribuir *software* malicioso que puede dañar sistemas o datos informáticos. En esencia, tal descripción de la casuística se subsume en el mismo tipo (art. 264 del CP) que la anterior conducta analizada con detalle y cuyos elementos, por ende, son similares.

En el contexto de los videojuegos, este delito puede consistir en distribuir virus, gusanos o troyanos que pueden robar información de los usuarios o dañar sus equipos. Encajaría en el tipo básico del 264 del CP, aunque habría que estar al supuesto concreto dado que existen tipos agravados dentro del mismo artículo.

Dentro del sector del videojuego cabe destacar que, en 2015, un grupo de personas fue condenado a penas de prisión de entre uno y dos años por distribuir *malware* (un tipo de virus informático)⁴⁵ a través de un videojuego. En concreto, la Sala de lo Penal de la Audiencia Nacional, dictó sentencia el 11 de junio de 2015⁴⁶, en la que consideró probados la infección de 23.662 ordenadores con un coste de reparación de 3,3 millones de euros. Se les condenó, finalmente, por un delito de daños continuados por la infección masiva de ordenadores mediante un sistema que se reproducía de forma automática para controlar y vigilar equipos informáticos con sus correspondientes indemnizaciones por responsabilidad civil⁴⁷.

En este sentido, y a nivel generalizado, es decir, no de forma explícita en los sectores de los videojuegos y de los deportes electrónicos, existe un escaso recorrido jurisprudencial de entre los que cabe destacar dos casos de distribución de *ransomware* en 2011. Uno de

40 GÓMEZ RIVERO, M. C. (2015). Nociones fundamentales de Derecho penal (Vol. II) Parte Especial. Tecnos, Madrid, pp. 198 y 199.

41 Debe entenderse programar en el sentido más informático del concepto, es decir, como definición de una lógica de ejecución o como proceso a aplicar cuando un determinado proyecto necesita del lenguaje informático.

42 GORJÓN BARRANCO, M.C. op. cit. pp. 102 y 103.

43 El Juzgado de lo Penal número 3 de Gijón, en su sentencia 385/2015, de 6 de Julio de 2016, absolvió a los tres acusados por falta de pruebas.

44 Información obtenida de diversos medios:

– Medio Computer hoy, disponible en: <https://computerhoy.com/reportajes/10-anos-hackeo-psn-nos-tuvo-casi-mes-poder-jugar-online-850979>. Última consulta: 27/01/2025.

– Medio Mundo Deportivo, disponible en: <https://www.mundodeportivo.com/alfabeta/playstation/sony-podria-haber-sido-hackeada-siendo-playstation-una-de-las-comprometidas>. Última consulta: 27/01/2025.

– Medio Gamer Focus, disponible en: <https://www.gamerfocus.co/juegos/expedientes-gf-el-gran-apagon-de-playstation-network/>. Última consulta: 27/01/2025.

45 Según la RAE: Programa introducido subrepticamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada.

46 Sentencia de la Audiencia Nacional (Sala de lo Penal) 17/2015 de 11 de junio de 2015.

47 Información disponible en: <https://noticias.juridicas.com/actualidad/jurisprudencia/10233-un-ano-de-carcel-para-tres-039;hackers039;-por-infectar-con-un-virus-a-mas-de-23-000-ordenadores-zombis/>. Última consulta: 23/01/2025.

los casos, conocido como “virus de la policía” por el *modus operandi* de los delincuentes⁴⁸. En este caso se solicitaba la aplicación del art. 264.2 entendiendo que el virus obstaculizaba o interrumpía el funcionamiento del sistema atacado.

En este sentido la ya referida Sentencia del Tribunal Supremo de 20 de mayo de 2022 indica que: “el art. 264 construye un tipo agravado para el caso en que los daños hayan sido “de especial gravedad” y el apartado 5 del mismo precepto incluye un tipo hiperagravado si “... los hechos hubieran resultado de extrema gravedad.”

V. DELITO DE DAÑOS INFORMÁTICOS EN LOS ESPORTS

Del mismo modo que ocurre en el ámbito de los videojuegos, en las competiciones de deportes electrónicos también pueden producirse conductas constitutivas de delito, ya sea durante su celebración o con anterioridad, afectando así a los elementos preparatorios que hacen posible la propia competición.

Para proseguir con el presente apartado, debe precisarse qué son los *eSports* y, para dar respuesta a esta cuestión se usa la definición proporcionada en el Libro Blanco del Deporte de la ya mencionada AEVI, al ser un organismo de España y al entender que el concepto se ajusta fielmente a la realidad del sector, puesto que la concepción de deporte electrónico ha evolucionado desde el origen⁴⁹ hasta la actualidad. La AEVI señala que *eSports* “es el nombre con el que popularmente se conocen a las competiciones de videojuegos estructuradas a través de jugadores, equipos, ligas, *publishers*, organizadores, *broadcasters*, patrocinadores y espec-

tadores. Se puede jugar de forma amateur o profesionalizada. Otras denominaciones son “gaming competitivo”, “organized play”, “egaming” o “pro gaming”⁵⁰.

Es preciso subrayar, asimismo, que, aunque todo *eSport* tiene como base un videojuego, no cualquier videojuego puede considerarse un *eSport*. Esta diferenciación obedece a varias razones que solo se apuntan de forma sucinta, dado que el análisis detallado excede la finalidad de este capítulo: la existencia de una dinámica competitiva articulada en torno al juego, la posibilidad de que las competiciones adopten tanto un formato de evento aislado como de liga estable, la necesidad de un sujeto que asuma la organización del certamen, la orientación de la actividad hacia la obtención de una victoria o recompensa concreta y, finalmente, la separación nítida entre jugadores individuales y estructuras de equipo⁵¹.

Del mismo modo que en el anterior apartado, no se pretende hacer una compilación *numerus clausus* de los delitos y supuestos existentes en el sector, sino que se trata de recoger aquellos supuestos que más destacan por sus particulares características y su vinculación con los entornos digitales y profesionalizados.

Existen diversas formas de materializar estos actos en el sector de los deportes electrónicos, una de ellas es atacar los servidores de la competición que se está desarrollando en un momento y lugar preciso y, de este modo, provocar un apagón o una interrupción del servicio. Esto podría llegar a impedir que los jugadores compitan o que los espectadores vean el desarrollo de la competición, produciendo un evidente detrimento tanto económico como social para todas las partes implicadas, organizadores, patrocinadores, espectadores, jugadores, etc⁵².

48 En este sentido, se considera interesante transcribir el mensaje utilizado por los ciberdelincuentes tal y como se pone de manifiesto en los Hechos Probados tanto de la Sentencia de la Audiencia Nacional (Sala de lo Penal) 14/2016, de 3 de marzo de 2016 como en la Sentencia de la Audiencia Nacional (Sala de lo Penal) 28/2016, de 4 de julio de 2016, “En los sistemas atacados aparecía el siguiente mensaje: “La POLICIA ESPANOLA. Atención!!! Ha sido detectada actividad ilegal!!! Su sistema operativo ha sido bloqueado debido a una infracción de la legislación española! Han sido detectadas las siguientes infracciones: Su dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la difusión de la pornografía infantil, zoofilia e imágenes de violencia contra menores! En su ordenador han sido detectados los archivos de video de contenido pornográfico con elementos de violencia y pornografía infantil! Además, desde su ordenador se realiza un envío ilegal (SPAM) de orientación pro terrorista. El presente bloqueo ha sido realizado para prevenir la posibilidad de difusión de dichos materiales desde su ordenador en Internet. Para desbloquear su ordenador, usted debe pagar una multa de 100 euros! La multa tiene que ser pagada antes de 24 horas desde el momento del bloqueo de su ordenador! En el caso de impago, todos los datos de su ordenador serán eliminados!”.

49 Cabe destacar la que se considera como una de las primeras definiciones modernas de los *eSports*, la ofrecida por Wagner que lo entiende como “un área de las actividades deportivas en la que las personas desarrollan y entrenan habilidades mentales o físicas en el uso de las tecnologías de la información y la comunicación”. WAGNER, M. G. ‘On the scientific relevance of eSport’, Proceedings of the 2006 International Conference on Internet Computing and Conference on Computer Game Development, 2006, pp. 437-440.

50 Libro Blanco de los Esports en España, Asociación Española de Videojuegos, p.9. Disponible en: https://www.aevi.org.es/web/wp-content/uploads/2018/05/ES_libroblan-co_online.pdf. Última consulta: 14/02/2025.

51 IAB SPAIN, Libro Blanco de los esports, 2021.

52 Cfr. GARCÍA CARMONA, D. (2025). “Nuevas realidades: la incidencia del Derecho Penal en los deportes electrónicos o eSports”. En Abadías Selma, A. y Guillén Pajuelo, Á. (coords.). *Delitos en el deporte: un enfoque jurídico contemporáneo*. Tecnos. Madrid, pp. 276 y ss.

Ahondando un poco en este supuesto de hecho, puede quedar subsumido en el art. 264 del CP⁵³ ya que se altera un programa informático, pero podría entenderse recogido en el art. 264 bis del CP debido a que, de facto, interrumpe de manera grave un sistema informático ajeno pues, dicha acción impide que se lleve a cabo la retransmisión de la competición a la que han accedido miles de espectadores⁵⁴.

Este encaje penológico tiene relevancia porque el art. 264 bis del CP citado prevé unas penas mayores a su tipo nuclear, de hecho, entendiendo la interrupción de una competición profesional en directo como un daño o una inutilización de un sistema informático se contemplan penas de 3 a 8 años de prisión, pena muy superior a la del tipo básico del 264 de 6 meses a 3 años.

Además del caso anterior, existen otros supuestos en los que los ciberdelinquentes atacan no a servidores generales en concreto para bloquear e interrumpir el porvenir de una competición en directo, sino que atacan el ordenador o consola de los jugadores profesionales produciendo, por ejemplo, un sobrecalentamiento de estos dispositivos electrónicos incrementando la cantidad de energía que llega a ellas para provocar, de este modo, daños materiales e informáticos⁵⁵.

Del mismo modo, se dan ataques directos a los *gamers* o jugadores profesionales, pero no para sobrecalentar los dispositivos e impedir su participación activa en la competición, sino que, en este caso, los ciberdelinquentes, normalmente usan un *ransomware*⁵⁶ para bloquear determinados perfiles en videojuegos concretos y guardar datos para luego exigir un rescate⁵⁷.

Tal y como apunta VERDUGO GUZMÁN, “también existen casos de videojugadores que han sufrido el secuestro de credenciales, contraseñas y cuentas, que contienen los avances en sus videojuegos o bienes

digitales adquiridos en plataformas que utilizan en el ciberespacio para jugar profesionalmente”⁵⁸.

Si bien es cierto que, en el primero de los primeros supuestos, puede quedar subsumido en el tipo básico del 264 CP, y que el segundo caso, el del uso de un virus, puede tener también su encaje en el tipo del art. 264 bis puesto que puede interrumpirse el funcionamiento de un sistema informático ajeno inutilizándolo o dañándolo, habrá que estar al caso en concreto y consecuentemente a la gravedad de las acciones.

Hasta ahora, con independencia del encaje penal en el tipo concreto, los ilícitos referidos tienen en común al *gamer* o jugador profesional como uno de los sujetos pasivos⁵⁹, es decir, aquella persona contra la que se comete la acción reproducible penológicamente. Si se cambia este enfoque y se pone a estos *gamers* como sujetos activos del tipo, podemos analizar otra forma de cometer un ilícito en las competiciones de deportes electrónicos. De igual manera, estas acciones podrían realizarse tanto antes como durante la competición.

Tomando de nuevo como base el delito de la alteración de datos, podría suceder que, un jugador, o un tercero por encargo de este “ataque” los ordenadores o consolas de otros jugadores y modificar el *software* o los datos del juego lo que podría desembocar en proporcionar a un determinado jugador una ventaja injusta sobre sus oponentes o, en la situación inversa, suponerle un detrimento para competir. Si bien es cierto que, en ese caso, habría que valorar según la afectación al bien jurídico el régimen de responsabilidad del jugador profesional de deportes electrónicos,

Este supuesto tendría su cabida penológica en el tipo nuclear con la acción “alterar” datos informáticos. En el contexto de los deportes electrónicos, este delito puede consistir en modificar los datos de un videojuego para obtener una ventaja competitiva injusta, como

53 Se precisa que, puesto que se ha hecho con anterioridad para este precepto, no se va a reproducir de nuevo aquellas cuestiones más puramente penales sobre la teoría del delito.

54 Ejemplos ilustrativos de ello son las finales de los videojuegos de Counter Strike del año 2021 en Estocolmo, Suecia, que contó en sus últimas ediciones con más de dos millones de espectadores y de *League of Legends*, también del año 2021 y celebrada en Reykjavik, Islandia que contaron con más de cuatro millones de espectadores. Información disponible en: <https://www.infobae.com/america/tecnologia/2021/11/08/historica-cifra-de-asistentes-a-las-finales-de-esports-de-league-of-legends-y-counter-strike-global-offensive/>. Última consulta: 10/01/2025.

55 VERDUGO GUZMÁN, S. (2023). *Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos*, Tirant lo Blanch, Valencia, p. 142.

56 El *ransomware* es un tipo de *malware* que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. Definición aportada por: *Instituto Nacional de Ciberseguridad (España)*, “Aprende Ciberseguridad”. Disponible en: <https://www.incibe.es/aprendeciberseguridad>. Última consulta: 14/02/2025.

57 En este sentido se pronuncia VERDUGO GUZMÁN, S. (2023). *Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos*, op. cit., p. 138.

58 VERDUGO GUZMÁN, S. (2023). *Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos*, op. cit., p. 142.

59 Existen, por extensión de lo señalado, otros sujetos pasivos en el sector de los *eSports*, como organizadores, inversores, *publishers*, etc.

mejorar o empeorar las estadísticas de un personaje, o conseguir objetos o recursos de manera ilegal⁶⁰.

VI. OTRAS MODALIDADES DELICTUALES EN LOS VIDEOJUEGOS Y EN LOS ESPORTS: ESPECIAL REFERENCIA A LA PROPIEDAD INTELECTUAL

En este apartado se manifiestan diversos delitos, que, por las características y particularidades de los deportes electrónicos, se consideran de especial relevancia en el referido sector.

En este sentido, uno de los ámbitos especialmente afectados por la comisión de ilícitos en el entorno de los videojuegos es el de la propiedad intelectual, tal y como se ha señalado con anterioridad. Ello, pese a los esfuerzos del legislador que ha venido modificando el CP para realizar una mayor aproximación al contenido dispuesto en el Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril (TRLPI o LPI). Estas modificaciones han tenido la finalidad de prevenir conductas que vulneren los derechos de autor a través de las nuevas tecnologías aprovechando las posibilidades que ofrece internet⁶¹.

Los videojuegos son una obra intelectual en cuanto a que reúnen las características de originalidad y expresión que se requieren en el TRLPI y por ello se han de considerar creaciones originales susceptibles de protección. Aunque el TRLPI no recoge a los videojuegos en el listado ejemplificativo de obras originales hallado en el art. 10 del citado texto, el posicionamiento doctrinal mayoritario es de considerar a los videojuegos como obras de autoría compleja⁶² compuesta a su vez por varias obras protegibles por los derechos de autor⁶³.

Los videojuegos se enfrentan, como sector, a la piratería⁶⁴ como mayor óbice para seguir consolidándose

como una de las grandes industrias mundiales y como ejemplo paradigmático de delito contra la propiedad intelectual.

Del mismo modo que se ha hecho con el análisis del delito de daños en su vertiente informática, y con ello poniendo de relieve la realidad práctica y la necesidad de profundizar en este tipo penal concreto, cabe traer a colación el bloqueo de más de sesenta páginas web vinculadas al dominio *ThePirateBay* por parte de la Comisión Antipiratería del Ministerio de Cultura, dado que se trataba de una de las principales plataformas de difusión ilícita de contenidos multimedia⁶⁵.

Para hacerse una idea del perjuicio que este ilícito produce en la industria se toman los datos publicados por el Observatorio de piratería y hábitos de consumo de contenidos digitales que, en su estudio de 2022 cifró las pérdidas de la industria de los videojuegos en 159 millones de euros en España⁶⁶.

Con el fin de seguir aportando datos que evidencian la frecuencia y relevancia de esta forma de criminalidad, resulta pertinente mencionar una reciente resolución del Juzgado núm. 9 de Valencia relativa a uno de los asuntos más notorios de los últimos años. En dicha sentencia se condena a la mercantil Alvisis Internet S.L. y a su administrador único a una pena de prisión y al abono, de forma conjunta y solidaria, de una indemnización de 15.000 euros a la Asociación Española de Videojuegos (AEVI, en lo sucesivo) por la comisión de un delito de piratería. La condena se fundamenta en que la empresa facilitaba el empleo de copias no autorizadas de videojuegos mediante la comercialización de diversos dispositivos electrónicos, además de ofrecer servicios de modificación de consolas destinados a neutralizar los sistemas de protección incorporados por distintas plataformas.

A través de una página web específica, el condenado distribuía dispositivos destinados a piratear múltiples

60 Por supuesto, esta acción ilícita también podría realizarse por otro sujeto que no fuese un jugador, pero, en este caso, se pretender dar a conocer potenciales acciones reprobables en el que el sujeto activo sea el propio *gamer*.

61 RODRÍGUEZ-VÁZQUEZ, V. (2019). «Los ciberdelitos contra la propiedad intelectual ¿cambiar todo para que nada cambie?: del ánimo de lucro al de obtener beneficio económico directo o indirecto», *Revista Electrónica de Ciencias Criminológicas*, núm.4, p.4.

62 El Tribunal de Justicia de la Unión Europea, en el Considerando 23 de su sentencia de 23 de enero de 2014, asunto C-355/12 Nintendo y otros, define a su vez a los videojuegos en consonancia con la doctrina como un material complejo compuesto de un programa de ordenador, diversos elementos gráficos y sonoros.

63 WILLEN GROSHEIDE, F., ROERDINK, H. & THOMAS, K. (2014). «Intellectual Property Protection for Video Games. A View from the European Union». *Journal of International Commercial Law and Technology*, Vol. 9, Num. 1, pp. 9 y 10 y DELGADO GARCÍA-POMAREDA, J. «De Víctor Hugo al Fornite: nuevas funciones para las entidades de gestión colectiva en el ámbito de los e-sports». En ORTEGA BURGOS, E. (dir.). *Propiedad Intelectual 2021*. Valencia. Tirant Lo Blanch, 2021, p. 90.

64 Debe entenderse la piratería como la infracción de los derechos de autor de los creadores de videojuegos. Normalmente consiste en la copia y ulterior distribución del *software* de un videojuego a través de páginas de acceso abierto.

65 Información obtenida en: <https://www.lavanguardia.com/cultura/20190624/46307-8138695/gol-pe-pirateria-bloqueo-webs-thepiratebay.html>. Última consulta: 14/02/2025.

66 Este estudio se lleva a cabo por CEDRO (Centro Español de Derechos Reprográficos. Se trata de una asociación sin ánimo de lucro que representa y defiende colectivamente los derechos de propiedad intelectual de carácter patrimonial de los autores y editores de obras textuales protegidas (libros, revistas, periódicos y partituras musicales).

consolas, entre ellas, Sony PS2 y PS3, así como Xbox 360, entre otras. Con dichos instrumentos y servicios de modificación lograba superar las medidas tecnológicas de seguridad integradas en los sistemas, permitiendo la reproducción ilícita de videojuegos y el almacenamiento de copias ilegales en tarjetas de memoria. Junto a su propio sitio web, el autor utilizaba plataformas adicionales como Amazon, Wallapop o Aliexpress para comercializar este tipo de dispositivos⁶⁷.

De igual modo, una vez vista la existencia de estos tipos delictuales y evidenciando casos acontecidos, procede analizar con cierto detalle algunos aspectos de la teoría del delito en cuanto al tipo contra la propiedad intelectual.

Uno de los elementos más controvertidos del tipo es el referente al bien jurídico puesto que existen tres vertientes o posicionamientos doctrinales dominantes al respecto que se tratan de sintetizar en las siguientes líneas:

- La vertiente patrimonialista que se base en la ubicación sistemática del precepto dentro del CP⁶⁸.
- La vertiente personalista que prima la prioridad de la tutela de las facultades morales vinculando la propiedad intelectual con el derecho fundamental a la producción y creación literaria, artística, científica y técnica del art. 20.1.b de la Constitución Española⁶⁹.
- La vertiente mixta que apuesta por una protección penal equitativa tanto de las facultades personales como de las patrimoniales⁷⁰.

Se trata de un delito común en cuanto a que para su comisión no es preceptiva ninguna cualidad o condición específica⁷¹. Si bien es cierto que, de igual forma, al anterior ilícito analizado ha de producirse sobre algo ajeno y sin consentimiento⁷².

En cuanto al objeto material del ilícito ha de destacarse que se trata de una norma penal en blanco en cuanto

a que es necesario acudir a lo dispuesto en el TRLPI para entender ciertos conceptos como son obra⁷³ y prestación literaria. En este sentido los *eSports* en cuanto a que son videojuegos quedan englobados en el tipo y en consecuencia están bajo la protección del mismo.

De igual modo, para dilucidar los aspectos concernientes a la acción típica que se recoge en el tipo básico del art. 270 del CP, en concreto, quien reproduzca, plagie, distribuya, comunique públicamente o explote económicamente habrá que estar a lo que indique la normativa específica, es decir, a lo que se contenga en el TRLPI.

Por supuesto, además de las anteriores conductas que se han tratado con cierta profundidad y detenimiento por considerarse como algunas de las más relevantes por diferentes motivos, como puede ser el impacto socioeconómico, existen muchas otras actividades susceptibles de reprobación penal en el entorno de los videojuegos y que, de forma breve y sin ánimo de configurar un glosario *numerus clausus*, interesa resaltar, nuevamente por su relevancia y, por desgracia, por su reiteración en el entorno que se está analizando.

Cabe precisar que las actividades o acciones que se van a exponer a continuación, así como sus definiciones han sido facilitadas por el Instituto Nacional de Ciberseguridad de España⁷⁴:

Cybersquatting, o apropiación de nombres de dominio, consiste en registrar un determinado nombre de dominio que simula a uno legítimo, para posteriormente utilizarlo con fines fraudulentos.

Grooming, es una práctica en la que un adulto se hace pasar por un menor en internet o intenta establecer un contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales.

La Ingeniería social, es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario

67 Información disponible en <https://www.audiovisual451.com/la-justicia-espanola-dicta-una-nueva-sentencia-contra-la-pirateria-en-el-sector-del-videojuego/>. Última consulta: 14/02/2025.

68 POLAINO NAVARRETE, M. (1989). "Los delitos contra la propiedad intelectual en la reforma penal española". *Criminología y Derecho penal al servicio de la persona* (Libro homenaje al Profesor Antonio Beristain). Instituto Vasco de Criminología, San Sebastián, pp. 869 a 872.

69 ROLDÁN BARBERO, H. (1988). *Personalismo y patrimonialidad en la reciente modificación de los delitos contra los derechos intelectuales*. T.II, La Ley, Madrid, pp. 912 a 922.

70 LATORRE LATORRE, V. (1994). *Protección Penal del derecho de autor*, Tirant lo Blanch, Valencia, pp. 126- 131.

71 TIRADO ESTRADA, J.J. (2016). Los delitos contra la propiedad intelectual tras la reforma del código penal de 2015. En Fayos Gardó, A. *La propiedad intelectual en la era digital*, Dykinson, Madrid, p. 344.

72 SANCHIS CRESPO, C. y VELASCO NÚÑEZ, E. (2019). *Delincuencia Informática*. Tirant lo Blanch, Valencia, p. 70.

73 En este caso, se ha de estar a lo dispuesto en los arts. 10 (Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: Después, el precepto hace una enumeración *numerus apertus* de lo que se considera como tal.) a 12 del TRLPI en consonancia con el art. 21 y sensu contrario con el art. 13 puesto que este último indica qué no es objeto de propiedad intelectual.

74 Instituto Nacional de Ciberseguridad (España), "Aprende Ciberseguridad". Disponible en: <https://www.incibe.es/aprendeciberseguridad>. Última consulta realizada el: 14/01/2025.

y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios *web* fraudulentos.

En estas competiciones de deportes electrónicos en directo se pueden cometer, por parte tanto de los competidores profesionales como de los espectadores, otros tipos de ilícitos que merece la pena traer, de forma breve y sucinta, a colación ya que se pueden cometer en este ámbito y por medios informáticos necesariamente como, por ejemplo, el supuesto en el que un espectador utiliza un *bot* para enviar mensajes de *spam* o de odio en el chat público en el que se retransmite una competición.

También podrían darse delitos de acoso y ciberacoso. Estos delitos pueden consistir en amenazas, insultos, humillaciones o cualquier otra conducta que pueda causar daño moral o psicológico a la víctima.

Incluso pueden darse casos de estafas y fraudes. Poniéndolo en contexto, estos delitos pueden consistir en la venta de entradas falsas para un evento en concreto, hechos subsumibles en el delito estafa informática del art. 249 CP, la obtención de datos personales de los espectadores o incluso de los *gamers* o la propagación de información falsa.

Igualmente, se pueden cometer por medios informáticos, calumnias e injurias hechas con publicidad informática (art. 211 CP), uso de cualquier equipo terminal de telecomunicación sin consentimiento de su titular (art. 256 CP), delitos informáticos contra la propiedad intelectual (art. 270 CP), propiedad industrial (arts. 273 y 274 CP), espionaje empresarial (arts. 278 y 279 CP)⁷⁵.

Continuando con estas tipologías delictuales cabe resaltar e incidir en ella de una forma un poco más profunda a las conductas analizadas en párrafos anteriores de este apartado, las apuestas, de las que se ha registrado algún caso, hace una década, aunque en EE.UU.: “Así, en 2014, se descubrió que en una de las competiciones americanas más importantes de Counter-Strike: Global Offensive (CEVO), varios de los jugadores de los equipos iBUYPOWER y NetcodeGuides.com pactaron el resultado de la partida que les enfrentaba, optando con ello a obtener más de 10.000 dólares en skins del mismo videojuego. La consecuencia fue la expulsión de los jugadores implicados por parte de Valve, propietaria del Counter-Strike: Global Offensive, de todas las competiciones patrocinadas por ellos”⁷⁶.

Una cuestión jurídica de relevancia es plantear la cabida jurídica que tendrían estas acciones en nuestro CP puesto que, *a priori*, todo induce a pensar que tendrían su cabida en el art. 286, *bis* 4, como corrupción en el deporte, en el sentido de que empleados, en este caso, jugadores profesionales de clubes de deportes electrónicos tienen por finalidad predeterminar o alterar de manera deliberada y fraudulenta el resultado de una prueba, encuentro de especial relevancia económica. No obstante, todo parece indicar que no sería por esta vía debido a que las competiciones de deportes electrónicos no se tratan de una competición deportiva pues, al menos en España los *eSports* no están considerados como deporte⁷⁷ ni como modalidad deportiva.

Además, se pone de manifiesto la especial dificultad de la carga probatoria en estos supuestos debido a que, en un deporte tradicional, como puede ser el fútbol, se puede entender que alguien se ha dejado marcar un gol. Sin embargo, en una competición de *eSports* como, por ejemplo, una final mundial, un partido en fase clasificatoria o un partido en una liga profesional del LOL, puede resultar complicado explicar que las acciones de un jugador se han realizado premeditadamente para dejarse vencer.

Entre las conductas ilícitas emergentes asociadas a los videojuegos conectados en línea y a los entornos de retransmisión en directo destaca el denominado *swatting*⁷⁸, una práctica que, aunque pueda aparecer revestida de un carácter lúdico o provocador, presenta una potencialidad lesiva extraordinariamente elevada. Esta conducta consiste en la realización de llamadas o avisos telemáticos falsos a las fuerzas y cuerpos de seguridad o a otros servicios de emergencia, en los que se comunica la existencia de un incidente grave inexistente tales como secuestros, situaciones con rehenes, atentados o amenazas con armas con la finalidad de provocar una intervención policial inmediata en el domicilio o localización de la víctima. Su origen y difusión se encuentran estrechamente vinculados a comunidades de jugadores jóvenes que interactúan en videojuegos online competitivos y plataformas de *streaming*, operando de manera funcionalmente análoga a los entornos de redes sociales.

Desde una perspectiva criminológica, el *swatting* constituye una forma específica de violencia digital indirecta, en la que el sujeto activo no ejecuta materialmente la agresión, pero instrumentaliza la reacción

75 FERNÁNDEZ BERMEJO, D. y MARTÍNEZ ATIENZA, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Thomson Reuters Aranzadi, Cizur Menor (Navarra), pp. 156 y 157.

76 *Guía Legal sobre los e-Sports*, op. cit., p. 25.

77 PALOMAR OLMEDA, A. y TEROL GÓMEZ, R. (2017). *Régimen jurídico de las competiciones de videojuegos. La necesidad de un marco jurídico para los videojuegos en España*. Difusión Jurídica, pp. 15-19.

78 Cfr., en detalle, CÁMARA ARROYO, S. (2023). «De las agresiones en el entorno escolar a la violencia digital: el cyberbullying en el derecho penal y la criminología». *Anuario de la Facultad de Derecho UAH*, Núm. 16, pp. 110 y ss.

coercitiva del Estado como mecanismo de daño. La conducta se ve facilitada por las características propias del entorno digital tales como anonimato, distancia física respecto de la víctima, desinhibición y percepción subjetiva de impunidad. Estas variables se intensifican en el ecosistema de los videojuegos online, donde la rivalidad competitiva, la exposición pública del jugador retransmitido y la lógica de la provocación generan un caldo de cultivo propicio para la banalización del riesgo. El resultado es una externalización del daño hacia el mundo físico, en la que la violencia institucional, legítima en su origen, se activa sobre la base de un engaño deliberado, produciendo situaciones de extremo peligro para la vida y la integridad de la víctima y de terceros.

El *swatting* ilustra de forma paradigmática la interrelación bidireccional entre ciberespacio y realidad física, al tratarse de una conducta iniciada en un entorno digital que despliega sus efectos más graves fuera de él. No se trata, por tanto, de una mera prolongación del ciberacoso, sino de un escalón cualitativamente distinto en la intensidad del ataque, en la medida en que introduce un riesgo inmediato y no controlado, susceptible de derivar en lesiones graves o incluso en la muerte. Ello obliga a descartar cualquier interpretación trivializante de la conducta y a situarla dentro de las manifestaciones más graves de agresión mediada tecnológicamente.

Desde el punto de vista dogmático, el ordenamiento penal español dispone de instrumentos suficientes para su represión sin necesidad de recurrir a nuevas figuras delictivas. Con carácter general, la conducta descrita presenta un encaje claro en el delito de falsa alarma del artículo 561 del Código Penal, al consistir en la comunicación falsa a servicios de emergencia con la consiguiente movilización de recursos públicos y alteración grave del orden público. El bien jurídico protegido no se limita al correcto funcionamiento de los servicios de seguridad, sino que se proyecta también sobre la seguridad colectiva y la confianza institucional. En aten-

ción a las circunstancias concretas del caso, no puede descartarse la concurrencia de otros tipos penales, en concurso real o ideal, cuando se produzcan resultados lesivos adicionales o se aprecien otros ataques autónomos a bienes jurídicos personales.

En definitiva, el *swatting* confirma que los videojuegos y los *eSports* constituyen un entorno de riesgo cualificado, no solo para la comisión de delitos informáticos o patrimoniales, sino también como escenario de manifestaciones extremas de violencia digital. Su análisis refuerza la necesidad de una aplicación rigurosa y sistemática del Derecho penal existente, evitando soluciones excepcionalistas, pero reconociendo la gravedad específica de aquellas conductas que, bajo la apariencia del juego o la provocación, instrumentalizan el poder punitivo del Estado como arma contra terceros.

Finalmente, se considera preciso y de relevancia hacer una expresa mención dentro del sector de los videojuegos y *eSports* a una tipología delictual especialmente sensible por el sujeto pasivo, se trata de la captación de menores para organizaciones criminales. El mundo del crimen organizado también se aprovecha del sector de los videojuegos para seguir nutriendo de activos sus filas. Hace eco de este problema plataformas como “Insight crime”⁷⁹ o como el noticiario “Infobae”⁸⁰, al exponer el reclutamiento de personas a través de los videojuegos. El *modus operandi* consiste en que un miembro de la banda, en este caso, de cárteles de narcotraficantes, se hace pasar por un jugador más, normalmente, en videojuegos de armas caracterizados por ser de un contenido violento, e invita a otros jugadores normalmente menores⁸¹, a asistir a un evento con la finalidad de captarlos para su organización⁸².

Este último caso es alarmante, pues los menores son sujetos que merecen especial protección y hay velar siempre por su seguridad y correcto desarrollo. Si bien es imposible controlar lo que hacen en cada momento siempre será recomendable que un supervisor responsable garantice que los menores están haciendo un uso adecuado y saludable de este tipo de productos⁸³.

79 InSight Crime es un centro de pensamiento y un medio de comunicación sin ánimo de lucro que busca profundizar y enriquecer el debate sobre el crimen organizado y la seguridad ciudadana en América Latina y el Caribe, mediante la publicación constante de informes, análisis, investigaciones y sugerencias de políticas sobre cómo abordar los múltiples desafíos que estas problemáticas presentan. Información obtenida a través de: <https://insightcrime.org/es/quienes-somos/>. Última consulta realizada el: 14/01/2024.

80 Uno de los medios digitales líderes en habla hispana, sobre todo, con notoria presencia en países de América Latina.

81 Información disponible en: <https://insightcrime.org/es/noticias/carteles-mexico-usan-videojuegos-reclutar-menores/>. Última consulta realizada el: 14/01/2024.

82 Información disponible en: <https://www.infobae.com/america/mexico/2021/09/22/la-infiltracion-de-los-carteles-mexicanos-en-el-mundo-gaming-asi-reclutan-a-sus-sicarios-a-traves-de-videojuegos/>. Última consulta: 10/01/2025.

83 Es este mismo sentido se pronuncia VERDUGO GUZMÁN, S. (2023). *Derecho Deportivo. Realidades y fantasías del metaverso. Los videojuegos como un medio de comisión delictiva y de vulneración de datos personales*. Tirant lo Blanch. Valencia, p. 297., cuando manifiesta que: “en resumen, el escenario perfecto para la comisión de estos delitos gira en torno a la participación de niños y adolescentes mediante videojuegos, por lo que es importante una preocupación de los padres, tutores o curadores legales, de cara a controlar los riesgos a los que se enfrentaría un menor que puede ser víctima o el autor de algún delito digital a causa de un videojuego”.

VII. CONCLUSIONES

El análisis realizado pone de manifiesto que la criminalidad vinculada a los videojuegos y a los deportes electrónicos no exige, en términos generales, la creación de nuevas categorías dogmáticas ni la formulación de un Derecho penal excepcional para el entorno digital. Por el contrario, los principales problemas que se detectan en la persecución penal de estas conductas derivan, fundamentalmente, de dificultades de subsunción y de aplicación de tipos ya existentes, concebidos originariamente para contextos distintos, pero suficientemente flexibles como para abarcar los supuestos examinados.

En este sentido, el estudio de los delitos de daños informáticos evidencia que el núcleo de las controversias no reside en la tipificación, sino en la determinación del bien jurídico protegido y en la valoración de la gravedad penalmente relevante. La coexistencia de lecturas patrimonialistas e interpretaciones que enfatizan la seguridad informática como bien jurídico colectivo obliga a un esfuerzo de concreción en la aplicación del artículo 264 CP, especialmente en entornos como los videojuegos online, donde el daño no siempre se traduce en una pérdida económica directa, pero sí en un menoscabo funcional significativo del sistema o del servicio. La solución no pasa por ampliar el tipo penal, sino por una interpretación rigurosa y restrictiva de sus elementos, acorde con el principio de intervención mínima.

Algo similar ocurre en relación con los delitos contra la propiedad intelectual. La consideración del videojuego como obra compleja y la expansión de prácticas de piratería digital muestran que el marco penal vigente ofrece herramientas suficientes para la tutela de este bien jurídico, siempre que se evite una aplicación automática de los tipos y se atienda a la estructura concreta de los hechos. El análisis desarrollado permite afirmar que los problemas más relevantes se sitúan en el plano probatorio y en la delimitación de la conducta típica frente a usos meramente privados o socialmente tolerados, cuestiones que han sido objeto de atención específica a lo largo del trabajo y que no requieren una reformulación dogmática general.

Por lo que respecta a las denominadas “otras modalidades delictuales”, el examen del ciberacoso, de las conductas de hostigamiento digital y de prácticas como el *swatting* confirma que los videojuegos y los *eSports* actúan, en muchos casos, como entornos facilitadores o amplificadores de formas de criminalidad ya conocidas. Desde esta perspectiva, la respuesta penal no debe construirse sobre la excepcionalidad tecnológica, sino sobre la correcta identificación del bien jurídico lesionado en cada supuesto, la integridad moral, libertad, seguridad colectiva u orden público y la adecuada subsunción en los tipos correspondientes, como ocurre

con el delito de falsa alarma del artículo 561 CP en los casos de *swatting*.

De todo lo anterior se desprende que no resulta necesario ni oportuno plantear, en el marco de este trabajo, una revisión dogmática global del Derecho penal aplicable al entorno de los videojuegos. Las tensiones detectadas pueden resolverse a través de criterios interpretativos más precisos y coherentes, especialmente en lo relativo a la valoración de la gravedad del daño informático, la identificación del sujeto pasivo real y la diferenciación entre ilícitos meramente contractuales o disciplinarios y aquellos que merecen una respuesta penal.

El principal aporte del estudio consiste, por tanto, en mostrar que el fenómeno analizado no demanda una expansión del ius puniendi, sino una aplicación técnicamente depurada del Derecho penal existente, sensible a las particularidades de los entornos digitales, pero respetuosa con los principios de legalidad, proporcionalidad y ultima ratio. En este sentido, el trabajo aspira a contribuir a una mejor delimitación de los márgenes de intervención penal en un sector en expansión, evitando tanto la banalización de conductas potencialmente graves como la sobre-reacción punitiva ante realidades tecnológicamente novedosas.

VIII. BIBLIOGRAFÍA

- AAVV (2017). Estudio sobre la Criminalidad en España. Ministerio del Interior, Madrid.
- ANDRÉS DOMÍNGUEZ, A. C. (2015). «Comentario previo a los artículos 264, 264 bis, 264 ter y 264 quater». En: GÓMEZ TOMILLO, M. (dir.). Comentarios prácticos al Código Penal. Tomo III, Delitos contra el patrimonio y socioeconómicos. Aranzadi, Pamplona.
- ARRASCO ANDRINO, M. M. (2009). «El acceso ilícito a un sistema informático». En: ÁLVAREZ GARCÍA, F. J.; MANJÓN-CABEZA OLMEDA, A.; VENTURA PÜSCHEL, A. (coords.). La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea. Tirant lo Blanch, Valencia.
- CÁMARA ARROYO, S. (2023). «De las agresiones en el entorno escolar a la violencia digital: el cyberbullying en el derecho penal y la criminología». *Anuario de la Facultad de Derecho UAH*, Núm. 16, pp. 83-125. Disponible en: <https://ebuah.uah.es/dspace/handle/10017/60984?locale-attribute=es>.
- DE LA MATA BARRANCO, N. J.; HERNÁNDEZ DÍAZ, L. (2009). «El delito de daños informáticos: una tipificación defectuosa». *Estudios Penales y Criminológicos*, núm. 29, pp. 311-362. Disponible

- en: <https://dialnet.unirioja.es/servlet/articulo?codigo=3138794>.
- DELGADO GARCÍA-POMAREDA, J. (2021). «De Víctor Hugo al Fortnite: nuevas funciones para las entidades de gestión colectiva en el ámbito de los e-sports». En: ORTEGA BURGOS, E. (dir.). *Propiedad Intelectual*. Tirant lo Blanch, Valencia.
- FERNÁNDEZ BERMEJO, D.; MARTÍNEZ ATIENZA, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Thomson Reuters Aranzadi, Cizur Menor (Navarra).
- GALÁN MUÑOZ, A. (2019). *Daños informáticos*. FUOC, Barcelona.
- GARCÍA CARMONA, D. (2021). «Esports: Origen, presente y futuro». *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, núm. 19, pp. 109-117. <https://doi.org/10.18172/redur.5127>.
- GARCÍA CARMONA, D. (2025). «“Esports” o deportes electrónicos: un breve recorrido en la normativa nacional e internacional». En: MILLÁN GARRIDO, A.; RODRÍGUEZ TEN, J. (coords.). *La dimensión internacional del deporte*. Reus, Madrid.
- GARCÍA CARMONA, D. (2025). «Nuevas realidades: la incidencia del Derecho penal en los deportes electrónicos o eSports». En: ABADÍAS SELMA, A.; GUILLÉN PAJUELO, Á. (coords.). *Delitos en el deporte: un enfoque jurídico contemporáneo*. Tecnos, Madrid.
- García Carmona, D. (2026). *Riesgos delictivos en el entorno de los deportes electrónicos*. Tesis Doctoral. Universidad de La Rioja.
- GÓMEZ RIVERO, M. C. (2015). *Nociones fundamentales de Derecho penal. Parte Especial (vol. II)*. Tecnos, Madrid.
- GORJÓN BARRANCO, M. C. (2021). «Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista». *Revista de Derecho Penal y Criminología*, 3.ª época, núm. 25, pp. 77-124. <https://doi.org/10.5944/rdpc.25.2021.28405>.
- HERNÁNDEZ DÍAZ, L. (2009). «El delito informático». *EGUZKILORE*, núm. 23, San Sebastián, diciembre, pp. 227-243. Disponible en: <https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf>.
- LATORRE LATORRE, V. (1994). *Protección penal del derecho de autor*. Tirant lo Blanch, Valencia.
- MIRÓ LLINARES, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4396388>.
- MIRÓ LLINARES, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons, Madrid.
- MORALES GARCÍA, O. (2011). «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas». En: QUINTERO OLIVARES, G. (dir.). *La reforma penal de 2010: análisis y comentarios*. Aranzadi-Thomson, Madrid.
- ORTS BERENGUER, E.; ROIG TORRES, M. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, Valencia.
- PALOMAR OLMEDA, A.; TEROL GÓMEZ, R. (2017). *Régimen jurídico de las competiciones de videojuegos. La necesidad de un marco jurídico para los videojuegos en España*. Difusión Jurídica.
- PÉREZ ARIAS, J. (2021). «Cibercriminalidad: hacia la nueva realidad —virtual— del Derecho penal». *Revista Internacional de Doctrina y Jurisprudencia*, vol. 26, pp. 175-193. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=8231363>.
- POLAINO NAVARRETE, M. (1989). «Los delitos contra la propiedad intelectual en la reforma penal española». En: *Criminología y Derecho penal al servicio de la persona. Libro homenaje al Profesor Antonio Beristain*. Instituto Vasco de Criminología, San Sebastián.
- REQUEJO-PASSONI, W. (2024). «El dilema de las copias de seguridad en el delito de sabotaje contra datos informáticos en el Derecho penal español». *Revista de Internet, Derecho y Política*, núm. 41. Disponible en: <https://vlex.es/vid/dilema-copias-seguridad-delito-1053535123>.
- RODRÍGUEZ-VÁZQUEZ, V. (2019). «Los ciberdelitos contra la propiedad intelectual: ¿cambiar todo para que nada cambie? Del ánimo de lucro al de obtener beneficio económico directo o indirecto». *Revista Electrónica de Ciencias Criminológicas*, núm. 4.
- ROLDÁN BARBERO, H. (1988). *Personalismo y patrimonialidad en la reciente modificación de los delitos contra los derechos intelectuales. T. II. La Ley*. Madrid.
- ROMEO CASABONA, C. M. (1988). *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información*. Madrid, pp. 42 y ss.
- ROMEO CASABONA, C. (2006). *De los delitos informáticos al cibercrimen. El cibercrimen, nuevos retos*.

- jurídico-penales, nuevas respuestas político-criminales. Comares, Granada.
- SANCHIS CRESPO, C.; VELASCO NÚÑEZ, E. (2019). Delincuencia informática. Tirant lo Blanch, Valencia.
- TIRADO ESTRADA, J. J. (2016). «Los delitos contra la propiedad intelectual tras la reforma del Código Penal de 2015». En: FAYOS GARDÓ, A. (ed.). La propiedad intelectual en la era digital. Dykinson, Madrid.
- VERDUGO GUZMÁN, S. (2023). Ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos. Tirant lo Blanch, Valencia.
- VERDUGO GUZMÁN, S. (2023). Derecho deportivo. Realidades y fantasías del metaverso. Los videojuegos como medio de comisión delictiva y de vulneración de datos personales. Tirant lo Blanch, Valencia.
- WAGNER, M. G. (2006). «On the scientific relevance of eSport». En: Proceedings of the 2006 International Conference on Internet Computing and Conference on Computer Game Development, pp. 437-442. Disponible en: <https://www.scirp.org/journal/paperinformation?paperid=79703>.
- WILLEN GROSHEIDE, F.; ROERDINK, H.; THOMAS, K. (2014). «Intellectual Property Protection for Video Games. A View from the European Union». Journal of International Commercial Law and Technology, vol. 9, núm. 1, pp. 1-13. Disponible en: <https://media.neliti.com/media/publications/28815-EN-intellectual-property-protection-for-video-games-a-view-from-the-european-union.pdf>
- WEBGRAFÍA Y OTRAS FUENTES DE INFORMACIÓN**
- AEVI Asociación Española de Videojuegos, “Libro blanco de los esports en España”. Disponible en: https://www.aevi.org.es/web/wp-content/uploads/2018/05/ES_libroblanco_online.pdf
- BARBARÁ ARTIGAS, A. (s. f.). La ley alemana para facilitar los visados en los esports. Disponible en: https://www.alexbarbara.es/legislacion_visados_esports_alemania/.
- BARBARÁ ARTIGAS, A. (s. f.). La regulación jurídica de los deportes electrónicos en Corea del Sur. Disponible en: <https://www.alexbarbara.es/la-regulacion-juridica-de-los-deportes-electronicos-en-corea-del-sur/>.
- Comité Olímpico Español: Los primeros Juegos Olímpicos de eSports se celebrarán en Riad en 2027. Disponible en: <https://www.coe.es/noticias/detalle-noticia/NEW-413d0426-e546-4ea9-9d41-1f84ca80a242/los-primeros-juegos-olimpicos-de-esports-se-celebraran-en-riad-en-2027/>.
- CEDRO: “Observatorio de piratería y hábitos de consumo de contenidos digitales”, 2022.
- ConceptosJurídicos.com, “Delito informático”. Disponible en: <https://www.conceptosjuridicos.com/delito-informatico/>.
- CounterStrike.com, “EL E-SPORT MÁS LONGEVO”. Disponible en: <https://www.counter-strike.net/>.
- Eltiempo.com, “¿Qué es Counter Strike y cómo se juega Tome nota, gamer?”. Disponible en: <https://www.eltiempo.com/tecnosfera/videojuegos/counter-strike-que-es-y-como-se-juega-759072>.
- Esports bureau: La Esports World Cup atrae a más de 500M de telespectadores y Team Falcons se corona como primer campeón de clubes. Disponible en: <https://esportsbureau.com/la-esports-world-cup-atrae-a-mas-de-500m-de-telespectadores-y-team-falcons-se-corona-como-primer-campeon-de-clubes/>.
- Guía Legal sobre los e-Sports. Presente y futuro de la regulación de los e-Sports en España, edit. ONTIER -Liga Profesional de Videojuegos, edición 2018.
- IAB SPAIN, Libro blanco Esports, 2021.
- Infobae, “La infiltración de los carteles mexicanos en el mundo del gaming: así reclutan a sus sicarios a través de videojuegos”. Disponible en: <https://www.infobae.com/america/mexico/2021/09/22/la-infiltracion-de-los-carteles-mexicanos-en-el-mundo-gaming-asi-reclutan-a-sus-sicarios-a-traves-de-videojuegos/>.
- Infobae, “Histórica cifra de asistentes a las finales de eSports de League of Legends y Counter Strike: Global Offensive. Disponible en: <https://www.infobae.com/america/tecno/2021/11/08/historica-cifra-de-asistentes-a-las-finales-de-esports-de-league-of-legends-y-counter-strike-global-offensive/>.
- Insight Crime, “Carteles en México usan videojuegos para reclutar a menores”. Disponible en: <https://insightcrime.org/es/noticias/carteles-mexico-usan-videojuegos-reclutar-menores/>.
- Ispo.com, “Historia de los esports: Cómo empezó todo. Disponible en: <https://www.ispo.com/es/negocio-del-deporte/historia-de-los-esports-como-empezo-todo#:~:text=Pero%20el%2019%20de%20octubre,entre%20s%C3%AD%20en%20%22%C2%A1Spacewar!>
- Kaspersky, “La IA y el machine learning en la ciberseguridad: como determinarán el futuro”. Disponible en: <https://www.kaspersky.es/resource-center/definitions/ai-cybersecurity>.

LaVanguardia.com, “Golpe a la piratería con el bloque de”. Disponible en: <https://www.lavanguardia.com/cultura/20190624/463078138695/golpe-pirateria-bloqueo-webs-thepiratebay.html>.

Marca.com, “Antes de los esports: los primeros campeones de videojuegos de la historia”. Disponible en: <https://www.marca.com/videojuegos/otrosjuegos/2020/11/03/5fa11edc46163fa7508b462d.html>.

NEWZOO. *Global Esports & Live Streaming Market Report*. 2022.

NEWZOO, *Global Games Market Report*, 2023.

Newzoo, “Principales países y mercados por ingresos de videojuegos <https://newzoo.com/resources/rankings/top-10-countries-by-game-revenues>.”

Pablo Maza, “Los delitos tecnológicos en los videojuegos. Disponible en: <https://pabloomazaabogado.es/penal-tecnologico/delitos-informaticos-en-videojuegos/>.”

RAE, disponible en: <https://www.rae.es/>.

UNODC (E4J). Módulo 1: “Introducción a la Ciberdelincuencia”, 2019.

WEZENBEEK, R. (2022). «Reportaje: el nuevo paradigma del sector audiovisual». Bit. La revista profesional sobre tecnología y transformación digital, núm. 223. COIT y AEIT. Disponible en: <https://bit.coit.es/el-nuevo-paradigma-del-sector-audiovisual/>.

JURISPRUDENCIA

Tribunal Superior de Justicia de la Unión Europea (TJUE)

Sentencia del Tribunal Superior de Justicia de la Unión Europea de 23/01/2014. Asunto C-355/12. ECLI:EU:C:2014:25

Tribunal Supremo (TS)

STS 1520/2020 - ECLI:ES:TS:2020:1520

STS 528/2022 - ECLI:ES:TS:2022:528

Audiencia Nacional (AN)

Sentencia de la Audiencia Nacional (Sala de lo Penal) 17/2015 de 11 de junio de 2015. SAN 2034/2015 - ECLI:ES:AN:2015:2034

Sentencia de la Audiencia Nacional (Sala de lo Penal) de 3 de marzo de 2016. SAN 704/2016 - ECLI:ES:AN:2016:704

Sentencia de la Audiencia Nacional (Sala de lo Penal) 28/2016, de 4 de julio de 2016. SAN 2639/2016 - ECLI:ES:AN:2016:2639

Juzgado de lo Penal

Sentencia del Juzgado de lo Penal número 3 de Gijón, de 6 de Julio de 2016. SJP 39/2016 - ECLI:ES:JP:2016:39