REVISTA DE DERECHO PENAL, PROCESAL Y PENITENCIARIO

Director: *Esteban Mestre Delgado*

LA LEY penal

NÚMERO 141 AÑO 16 • NOVIEMBRE-DICIEMBRE 2019

ESTUDIOS MONOGRÁFICOS

«DELINCUENCIA CALLEJERA»

- Cuando los juegos se vuelven peligrosos. La criminalidad en los espacios virtuales multijugador
- La imprudencia menos grave: concepto y criterios para su correcta calificación jurídica tras las últimas reformas

Wolters Kluwer

DELINCUENCIA CALLEJERA

Editorial

Estudios monográficos

Temas de Actualidad

Legislación aplicada a la práctica

Jurisprudencia aplicada a la práctica

Derecho procesal

Derecho Penitenciario

Criminología

- Cuando los juegos se vuelven peligrosos. la criminalidad en los espacios virtuales multijugador, *Viviana Caruso Fontán*

Práctica penal

- La insolvencia parcial provocada del obligado al pago de pensiones del art. 227 CP, *Vicente Magro Servet*

Consultas de los suscriptores, *Carmelo Jiménez Segado*

- El patinete eléctrico en los delitos contra la seguridad vial
- La prueba ilícita

Criminología

Cuando los juegos se vuelven peligrosos. La criminalidad en los espacios virtuales multijugador (1)

Viviana Caruso Fontán

Profesora Contratada Doctora
Universidad Pablo de Olavide. Sevilla

FICHA TÉCNICA

Resumen: *El desarrollo de la tecnología y la expansión de internet han determinado el nacimiento de un nuevo tipo de delincuencia denominada «cibercriminalidad». Uno de los ámbitos en los que pueden desarrollarse estas conductas son los juegos en línea masivos multijugador. Se trata de mundos virtuales en los que interactúan los participantes, ya sea realizando tareas cotidianas, o bien dando vida a personajes fantásticos, pero en todo caso creando la posibilidad de que se reproduzcan, en estos universos, sucesos con capacidad para afectar en el mundo real a bienes jurídicos protegidos penalmente.*

Palabras clave: Abusos, Cibercriminalidad, Espacio virtual, Internet, Videojuegos.

Abstract: *The development of technology and the expansion of the internet have determined the existence of a new criminal kind called «cybercriminality». One of the areas in which these behaviors can be developed are massive multiplayer online games. These are virtual worlds in which participants interact either by performing daily tasks, or giving life to fantastic characters, but in any case creating the possibility of reproducing in these universes, events with the capacity to affect values protected by*

criminal law.

Keywords: Abuse, Cybercriminality, Internet, Videogames, Virtual space.

I. El contexto

Son las 10 de la noche de un lunes de mayo. Un grupo de personas confluyen en la sala de estar de una mansión en la que se está celebrando una fiesta. Entre ellos se encuentra un payaso gordo con cara de galleta, vestido con un atuendo de arlequín manchado de semen, ceñido con un cinturón de muérdago cuya hebilla lleva la inscripción «¡bésame debajo de esto, perra!». Entonces comienza el ataque: una violación comunitaria. Para ello el payaso, llamado Sr. Bungle, utiliza a un personaje vestido como una muñeca vudú, dirigiendo en primer término su atención a Starsinger, un personaje femenino bastante anodino, alto, robusto y de pelo castaño, obligándola a tener relaciones sexuales no deseadas con otros individuos presentes en la sala, entre ellos Bakunin, un conocido radical, y Juniper, una ardilla. Sus acciones se hacen cada vez más violentas, haciendo que Starsinger se viole a sí misma con un pedazo de un cubierto de cocina. Ninguno de los presentes lograba detenerlo hasta que llegó Zippy, un veterano sabio y de confianza, que trajo consigo un arma de poderes casi mágicos, un arma que no logró matar, pero sí envolver a sus objetivos en una jaula impermeable, logrando así detener los poderes de la muñeca (2) .

La valoración de estos sucesos, que normalmente daría lugar a estimar la concurrencia de varios delitos de violación, se ve alterada por el hecho de que nos encontramos ante una escena que tiene lugar en un mundo virtual. En concreto se trató de *LAMBADOO* y las víctimas admitieron haberse sentido sumamente indefensas y humilladas ante este ataque. Al tratarse de un juego virtual, podríamos llegar rápidamente a la conclusión de que estamos frente a una ficción y que, por tanto, las leyes que dirigen el comportamiento de los hombres no tienen nada que decir al respecto. Al fin y al cabo, no ha habido más que una interacción entre seres humanos y sus ordenadores, un simple accionar de teclas, no registrándose, en realidad, ningún contacto físico entre los participantes, que se encontraban en ese momento en distintos lugares del planeta. No obstante, esta conclusión no resulta tan obvia si alteramos alguno de los elementos de la historia: en una soleada mañana de junio, en un parque verde, una sonriente joven está siendo penetrada por dos personajes masculinos. Esta escena tiene lugar en el mundo virtual desarrollado para uno de sus juegos por la empresa *Roblox* y es descubierta por una madre que advierte horrorizada que, mientras lee un cuento a su niña de 7 años, ésta se encuentra observando cómo su personaje femenino sufre una violación sexual grupal por parte de dos varones en el juego de su *IPad* (3) . El hecho de que se encuentren involucrados menores de edad cambia radicalmente la percepción de los sucesos y nos indica que no resulta aceptable que el Derecho siga asumiendo una posición neutral, sólo por tratarse de sucesos que se desarrollan en mundos virtuales.

La criminalidad en los juegos en línea no afecta solamente a bienes jurídicos de carácter personal, como en los casos relatados anteriormente, sino que resulta muy habitual que se vean involucrados bienes de distinta naturaleza: un cazador de demonios se encuentra cruzando el puente de Aggramar cuando cae al vacío sin explicación alguna. Poco después descubre por sorpresa que se ha teletransportado instantáneamente, cayendo delante de un jefe de banda, al que además ha «pulleado» (provocado) de forma accidental. Este comportamiento no deseado es interpretado por los demás personajes de la banda como premeditado, por lo que deciden expulsarlo del grupo, perdiendo en consecuencia la posibilidad de acceder al contenido del máximo nivel de la expansión. Estas situaciones inexplicables se repiten indefinidamente hasta que un grupo de personajes se acerca al cazador de demonios para avisarle que sólo dejarán de utilizar la habilidad llamada «cambio», que les permite intercambiar las posiciones de sus personajes, en caso de que les entregue todo su oro. De esta manera, un jugador novato que lleva tiempo realizando tareas rutinarias para ver crecer en riquezas y capacidades a su personaje, accede a

entregar su oro a un grupo de jugadores veteranos para evitar que este acoso haga perder todas sus posibilidades de progresar en el juego. Veremos que las consecuencias que puede tener este hostigamiento en el mundo real no son sólo de carácter personal, sino también económicas, ya que el dinero virtual de los juegos resulta ser convertible a dinero real.

II. Juegos en línea masivos multijugador

La revolución que supuso la llegada de internet a nuestras vidas no se limitó a multiplicar nuestras posibilidades de comunicación y de obtención de información, sino que fue mucho más lejos, creando, incluso, mundos imaginarios paralelos. Los primeros videojuegos online que se popularizaron a finales del siglo pasado duraban sólo el tiempo que tardaba en trascurrir una partida, de forma que estos mundos virtuales acababan cuando el usuario apagaba el ordenador. Esto cambió de forma radical con la llegada de *Ultima Online.* Se trató del primer juego de rol multijugador masivo en línea, también llamados MMORPG, por las siglas de su nombre en inglés (*Massively Multiplayer Online Role Playing-Games*). A diferencia de los juegos anteriores, el universo de *Ultima Online* era persistente, de modo que, cuando el suscriptor se desconectaba, todo seguía existiendo, otros jugadores interactuando y las acciones propias y de otros tenían consecuencias perdurables para el momento en que se decidiera continuar la partida (4) . Según las palabras de sus creadores, se trata de un mundo creado para que vivan los personajes, un mundo que se ha desarrollado y aún se está desarrollando, expandiendo y creciendo todo el tiempo (5) .

Existen distintos tipos de juegos de rol de realidad virtual (6) :

— MMORPGS (juegos de rol multijugador masivos en línea): estos juegos tienen lugar en un mundo con cientos o miles de otros jugadores. Ejemplo de ellos, además del mencionado *Ultima Online*, es el mundialmente conocido *War of Warcraft*.

— MMOGS (juegos multijugador masivos en línea): son videojuegos que pueden soportar cientos o miles de jugadores al mismo tiempo. Permiten a los jugadores cooperar y competir entre sí a gran escala y, a veces, interactuar de forma significativa con personas de todo el mundo. Incluyen una variedad de tipos de juego, como la simulación de vuelo, simulación de gobierno y fantasía medieval. Ejemplos de los MMOG más populares son *Rune Scape, Utopia* y *Domain of Heroes*.

— MUVES (entornos virtuales multiusuario): se refieren a entornos virtuales multiusuario en línea. Los modernos tienen gráficos 3D en tercera persona, permiten la interacción simultánea del usuario, y representan un mundo virtual persistente. Ejemplos de los más populares son *Second Life*, *Doom* y *EverQuest*.

La creación de *Second Life* supuso una verdadera revolución. Se trata de una aplicación informática creada por la empresa *Linden Lab* que funciona como un programa cliente, esto es, se instala en los ordenadores de cada usuario y se conecta a los servidores de *Second Life*, una vez ejecutada. Tras su implantación, el usuario puede crear su avatar o alter ego para participar e interactuar en el mundo virtual, teniendo la capacidad de crear objetos y estructuras complejas y pudiendo realizar interacciones con otros usuarios (7) . En este juego no hay una misión concreta que cumplir, el único propósito es que el usuario pueda vivir aquella experiencia que en su día a día no puede. Para que el avatar creado por el jugador pueda obtener bienes debe pagar por ellos, de forma que *Linden Lab* ha creado una moneda que es convertible en dinero real. Mientras algunas compañías combaten con energía el intercambio de valores fuera del juego, ya que les traen más problemas que beneficios, otras lo facilitan. Este es el caso de *Linden Lab*, de forma que el Departamento del Tesoro de EEUU ha declarado al Dólar Linden «moneda virtual centralizada convertible». Existe una economía compleja basada en el comercio de bienes y servicios virtuales que se desarrolla de forma muy parecida a la realidad (8) . Los avatares tienen muchas formas de conseguir los dólares Linden, pueden comprarlos directamente en *Linden Lab* , ganarlos dentro del propio juego trabajando, creando objetos y vendiéndolos, mendigando, o poniendo en marcha negocios, entre muchas otras opciones (9) .

Este juego implicó toda una gran transformación de la forma de entender los mundos virtuales, particularmente durante los años 2006 y 2007. No obstante, el número de cuentas activas en

Second Life ha bajado significativamente en los últimos años (10) . Se ha sostenido que el auge de las redes sociales ha provocado que este mundo digital deje de tener sentido para las empresas anunciadoras. No obstante, el universo continúa con una gran comunidad de adeptos y sus creadores han recurrido a la tecnología de la realidad virtual 3D para crear *Sansar*, un nuevo mundo que es capaz de generar una sensación mucho más inmersiva y ser el sustituto de *Second Life*. En *Sansar* los usuarios pueden utilizar gafas como *Oculus Rift* para conectarse a un mundo digital, relacionarse con otras personas y desarrollar sus propias salas o visitar otras que ya se han diseñado (11) .

Por otro lado, en los MMORPGS no hay ganadores o perdedores, sino que se trata de hacer avanzar al personaje a lo largo de distintos niveles. *War of Warcraft* es, probablemente, el juego más exitoso de este tipo. En este mundo, el avance del personaje depende de la realización de tareas rudimentarias que permiten obtener oro para comprar objetos y poderes (12) . Puede tratarse de recoger el botín de los monstruos muertos, de hacer armas, pociones u objetos igualmente útiles para vender a otros jugadores o incluso de reunir las hierbas y los cueros y otros recursos que son las materias primas de los artesanos. Estas actividades y otras similares se conocen colectivamente como «la rutina», ya que resultan ser muy repetitivas y requieren que se les dedique largos períodos de tiempo para que supongan un avance significativo del personaje. Esta situación provocó que jugadores con un poder adquisitivo alto prefirieran pagar por la realización de estos trabajos, ahorrando tiempo y pudiendo ver a su personaje llegar a niveles altos rápidamente. De esta manera, pasó a utilizarse dinero real para comprar dinero u objetos del mundo virtual (13) .

En consecuencia, se inició una nueva actividad lucrativa denominada «agricultura del oro» (*Gold Farming*), desarrollada por trabajadores de países del tercer mundo que pasaban unas 12 horas delante del ordenador haciendo una y otra vez la misma tarea. Estas granjas de oro se encontraban en su mayor parte en China y explotaban a sus trabajadores, pagándoles una suma ínfima por su intensa jornada de trabajo. Nos estamos refiriendo a un negocio multimillonario de venta de efectivo virtual al instante (14) . A través de esta agricultura del oro, la economía virtual online se transformó en una economía del mundo real. Resulta relevante destacar que los jugadores tienen prohibido vender o comprar contenido generado a partir de *War of Warcraft*. Sobre esta situación no hay ambigüedad alguna, ya que los jugadores no tienen ningún derecho de propiedad sobre los objetos que son parte del juego. A pesar de ello, páginas web del estilo de e-Bay se convirtieron rápidamente en sitios populares para vender objetos virtuales (15) .

Con el tiempo, esta industria millonaria ha ido perdiendo sus elevados ingresos como consecuencia de las medidas de seguridad introducidas por las empresas desarrolladoras de los juegos. No obstante, ha surgido una nueva modalidad que ha reemplazado en parte al antiguo negocio. Se trata de lo que se ha dado en llamar «nivelación de potencia». Con esta opción, el usuario entrega los datos de su cuenta y el nivelador se encarga de elevar el personaje desde el nivel más bajo hasta el más alto, logrando en 4 semanas lo que a un ritmo normal llevaría 4 meses de trabajo (16) .

III. Mundos virtuales: ¿realidad o ficción?

Los mundos virtuales o metaversos son construcciones ficticias en las que los participantes interactúan a través de avatares creados por sí mismos tratando de reproducir la participación o vida real en un entorno de metáfora virtual sin las limitaciones espacio-temporales. Así, un metaverso hace referencia a un entorno 3D inmersivo (17) . Hasta hace poco, todos teníamos claras las diferencias que existían entre la realidad y la ficción. La ficción es simplemente una construcción imaginaria. Tal como pone de manifiesto AGUIRRE ROMERO, el concepto de virtualidad ha complicado las cosas, ya que lo virtual no es imaginario en la medida en que en los nuevos escenarios virtuales es posible realizar ciertas acciones que se acercan a una nueva forma de realidad. De tal manera, un mundo virtual es un espacio construido de forma deliberada y consciente para permitir el desarrollo de los seres humanos (18) .

En principio podría pensarse que la construcción «realidad virtual» resulta ser paradójica, ya que cada uno de los términos parece apuntar en direcciones lógicas contrarias. A pesar de ello, lo

cierto es que los espacios virtuales amplían la capacidad de comunicación de las personas. Son, por tanto, medios que permiten la convivencia y la construcción de relaciones de distinto tipo y grado (19) . Estos mundos virtuales desarrollados, en principio, para cumplir una finalidad de ocio, ya están teniendo aplicaciones muy diversas. Ejemplo de ello es la utilización de *Second Life* con finalidad educativa (20) o el simple hecho de que grandes multinacionales hayan creado «sedes» virtuales en este metaverso para promocionar sus negocios.

Los mundos virtuales, como especificidad del ciberespacio en el que se desarrollan, son espacios virtuales de interacción. Es posible sostener que el ciberespacio ha surgido «en» y «por» la comunicación, lo que le confiere una doble naturaleza de espacio y de medio. El ciberespacio es un espacio relacional cibernético en el que unas máquinas, que constituyen unas redes, sirven de medio para que se establezcan comunicaciones entre humanos. Como sostiene MIRÓ LLINARES, se trata de un tipo nuevo de espacio que es invisible a nuestros sentidos y en el que las coordenadas espacio-tiempo adquieren un significado diferente, ya que su alcance y sus límites se ven redefinidos (21) . De tal forma, el hecho de que no se requiera desplazamiento físico alguno para mantener un contacto multiplica las posibilidades de comunicación con múltiples sujetos en un período ínfimo de tiempo. De la misma manera, las características distintivas de este nuevo tipo de espacio también determinan que el factor tiempo se pueda ver alterado en otro sentido, ya que los actos pueden quedar fijados durante un tiempo indeterminado y seguir desplegando efectos aunque su ejecución haya durado solo un instante (22) . Es el caso de las opiniones vertidas en las redes sociales, que continúan siendo públicas de forma indefinida y que pueden seguir siendo visionadas por terceros multiplicando los efectos nocivos de un posible delito de injurias.

AGUIRRE ROMERO explica que el ciberespacio dirige sus acciones tanto hacia el interior como hacia el entorno. En el primer caso, el ciberespacio es utilizado como un medio para el cumplimiento de unos objetivos exteriores. En el segundo, permite la realización de objetivos sociales que se cumplen en el interior del propio sistema. Nos encontramos, por tanto, frente a un espacio de convergencia. Este es precisamente el caso de los juegos on-line, donde se desarrollan actividades que no pueden ser realizadas fuera del ciberespacio que servirá, en consecuencia, como espacio de encuentro. Así, el juego sucede exclusivamente en el ciberespacio y mientras éste dura los participantes están constituyéndose en una realidad virtual. Se trata de un subsistema dentro del sistema (23) .

IV. Cibercriminalidad: hacia un nuevo tipo de delincuencia

Todo lo dicho hasta el momento nos permite afirmar que estamos frente al nacimiento de un nuevo ámbito de comisión delictiva: el ciberespacio (24) y dentro de esta nueva realidad encontramos, a su vez, subsistemas con características muy particulares: los mundos virtuales creados para los juegos on-line. De ahí en más nos toca valorar cuál es el tratamiento jurídico que debe darse a esta nueva realidad.

Tal como sucede en cualquier ámbito que ofrezca la oportunidad de interacción entre los seres humanos, las nuevas oportunidades de relación y de desarrollo se ven opacadas por su utilización como un medio para el delito. En este sentido no hay, ni puede haber, diferencia alguna con respecto a otros campos de actividad. En nuestra opinión, es erróneo concebir al ciberespacio como un reino diferente al que los humanos pueden ingresar al abandonar el mundo real. A pesar de ello, no podemos negar que el ciberespacio reúne una serie de características definitorias que lo convierten en un fenómeno único, entre ellas se encuentran la deslocalización, transnacionalidad, descentralización, universalidad, así como también el carácter anónimo y popular (25) .

Estas particularidades han llevado a la doctrina a plantearse si estamos frente a una nueva categoría normativa de delitos para la cual puede ser necesario desarrollar nuevos principios jurídicos o bien si el ciberespacio es simplemente un medio que se utiliza para cometer delitos tradicionales. Se trata, por tanto, de determinar si existe en esta criminalidad diferencias materiales substanciales.

En este sentido se manifiesta POSADA MAYA, quien considera que no estamos frente a delitos tradicionales sino ante un tipo de delito especial, cuya riqueza técnica, su contexto virtual, la

afectación de objetos inmateriales y su localización en el ciberespacio rompen los esquemas teóricos y dinámicas probatorias propias de los delitos comunes. Así, este autor llega a hablar incluso del nacimiento de la «ciberacción» ya que, en sentido material, aunque estos comportamientos digitales tienen un origen en una acción-decisión humana, este movimiento sólo consiste en un «clic» que podría llegar a considerarse como un acto preparatorio del delito, mientras que los resultados no van a superar el mundo digital, pues se dan mediante el tratamiento, la manipulación y el almacenamiento de datos informáticos, que aunque representan materia y ubicación, realmente son sólo ondas de energía que forman bytes susceptibles de agruparse en archivos y que pueden ser leídos y traducidos por el sistema de signos comprensibles para los seres humanos (26) .

Para analizar esta problemática, BRENNER recurre al caso de la violación del Sr. Bungle ocurrida en la comunidad virtual *LAMBADOO*, ya relatada al inicio del presente trabajo. Así, en la opinión de esta autora, para que sea necesario crear una nueva categoría delictiva el sitio virtual donde sucede el crimen debe ponerlo fuera del alcance de los principios que se utilizan para imponer responsabilidad en el mundo real (27) . En este caso, uno de los jugadores se apoyó en la identidad de otros personajes e hizo que varios participantes femeninos realizaran actividades sexuales humillantes. Como consecuencia de estos actos, las víctimas quedaron traumatizadas y exigieron que la cuenta del causante fuera eliminada; por tanto, todos los elementos de la ofensa —excepto el sufrimiento de las víctimas y las pulsaciones sobre el teclado— ocurrieron en el ciberespacio. Durante el debate que se originó como consecuencia de estos actos se planteó si esta conducta debía ser juzgada exclusivamente dentro de la comunidad virtual o también por el sistema de justicia penal. En este sentido, se llegó a comparar el trauma sufrido por estas víctimas con el de una violación real. Resulta evidente que estos hechos no pueden dar lugar a un delito de agresiones sexuales en la medida en que no ha habido contacto corporal entre los participantes, pero tampoco puede negarse el impacto emocional que pueden haber sufrido las víctimas.

Si bien la mayor parte de los elementos de la ofensa ocurrieron en el ciberespacio, ello no implica que el lugar donde suceden los hechos sea lo que los ponga fuera de los principios que se utilizan para imponer responsabilidad en el mundo real. Lo que coloca a estos hechos fuera de la valoración de las normas penales es simplemente que no concurren los elementos típicos propios de los delitos de agresiones o abusos sexuales. La particularidad de desarrollarse en un mundo virtual no puede excluir una conducta del ámbito del Derecho, ya que no estamos frente a una ficción sino a una nueva forma de realidad. Situación diferente es que el hecho de desarrollarse en un mundo virtual dificulte la prueba o persecución de los delitos.

El hecho de que la conducta humana que se verifique en un ciberdelito se limite al accionar de las teclas de un ordenador no justifica que hablemos de unos meros «actos preparatorios». No estamos frente a un mero «clic», sino ante una conducta capaz de desencadenar un resultado que lesione o ponga en peligro bienes jurídicos. Muchas de las conductas que generan daños de gran entidad consisten únicamente en pequeños gestos: desde apretar un gatillo hasta detonar una bomba. Lo importante no es la simplicidad del gesto, sino el proceso que ese comportamiento puede desencadenar. En este sentido, entendemos que es erróneo ver al ciberespacio, y a su vez, a los mundos virtuales como una realidad diferenciada del mundo real. Por más complejos que sean los procedimientos informáticos que los originan, se trata de tecnología manejada por el hombre (28) .

En contra de esta postura, POSADA MAYA argumenta que el ciberdelito crea nuevas dinámicas criminales, ya que es posible instrumentalizar cadenas de víctimas que no tienen consciencia de que están siendo utilizadas para victimizar a terceros. Se trata, técnicamente, de ataques distribuidos mediante los cuales se utilizan automáticamente redes de computadores infectados (*Botnet*), sin conocimiento o con la complicidad de sus usuarios titulares, lo cual, desde la perspectiva del desvalor de acción objetivo, comporta una forma particular de ejecutar los delitos que facilita su comisión y la producción de sus efectos frente a la comunidad titular de los derechos a la disposición, el acceso y el tratamiento de información confiable e integral. Así ocurre, por ejemplo, en la suplantación de sitios web para capturar datos personales (29) .

Resulta indudable que la persecución y castigo de este tipo de conductas implican un desafío para juristas e investigadores y que requieren de nuevos medios y métodos de investigación, pero

no suponen necesariamente un replanteamiento de las estructuras penales. También en estos casos, la acción debe ser reconducida a la conducta humana voluntaria con la que se programan los equipos para dar lugar a esta cadena de resultados. En este sentido, los titulares de los equipos afectados que desconocen esta situación y que propagan el daño de forma inconsciente no serán más que instrumentos dentro del engranaje.

En esta materia, compartimos la opinión de MIRÓ LLINARES cuando señala que la clasificación de la cibercriminalidad resulta útil como categoría de base sociológica que sirva como referencia de un ámbito de riesgo que incluya todas las tipologías de comportamientos que utilicen la red para la realización de conductas que atenten contra bienes considerados esenciales. Esta categorización permitirá centrar los esfuerzos político-criminales para la lucha en contra de esta forma de criminalidad en aquellos aspectos que resultan necesarios, esto es, la adaptación de las estructuras procesales y técnicas necesarias para la prevención de su realización y la investigación más efectiva de las mismas (30) .

La creación de una categoría normativa de ciberdelitos resultaría abiertamente disfuncional debido a la gran variedad de bienes jurídicos que pueden ser atacados utilizando la red. Ello no obsta a que sea necesario crear algún delito que recoja conductas concretas que no puedan ser abarcadas por las ya existentes y que requieran por su gravedad de la intervención del Derecho penal. Así, BRENNER propone la creación de un delito que castigue la utilización de comunicaciones originadas por medio de un ordenador para infringir maliciosamente angustia emocional a alguien, tipo que, en su opinión, podría resultar aplicable en casos como el del Sr. Bungle (31) .

La doctrina también ha planteado la posibilidad de crear tipos cualificados que eleven la pena de los delitos comunes cuando se utilicen medios informáticos, electrónicos o telemáticos. Se trataría de que estos tipos cualificados recojan el aumento del desvalor de acción y de resultado que implica la utilización de medios que facilitan y favorecen la realización del delito y multiplican sus resultados. En esta línea, el legislador de 2015 incorporó un tipo cualificado al delito de incitación al odio o a la violencia racial, disponiendo que las penas «se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas» (art. 510. 3) (32) .

A continuación analizaremos las distintas infracciones que pueden llevarse a cabo en estas plataformas virtuales para tratar de determinar si el Código penal español se encuentra en condiciones de dar respuesta a estas situaciones o si puede ser necesaria la creación de nuevas figuras delictivas.

V. Delitos cometidos en mundos virtuales

1. Violación virtual

Tal como se ha argumentado anteriormente, atacar sexualmente a un personaje virtual no puede dar lugar a un delito de agresiones o abusos sexuales, ya que, para que se verifique una conducta propia de los artículos 178, 179 o 181 CP, es preciso que el ataque tenga una incidencia real sobre el cuerpo de la víctima. Así, a pesar de que el artículo 178 CP utiliza la técnica de definir la conducta típica a través de la lesión del bien jurídico «libertad e indemnidad sexuales», existe consenso en la doctrina a la hora de aceptar que la consumación del tipo requiere que la conducta involucre directamente el cuerpo de la víctima (33) . Esto no sucede ni en el caso del Sr. Bungle ni en el ataque efectuado al avatar de la niña de 7 años. No obstante, en este supuesto no puede descartarse que la afectación de la indemnidad sexual de la menor tenga relevancia suficiente como para dar lugar a un hecho delictivo, por lo que deberemos valorar la posible aplicación de otro tipo penal.

El artículo 183 bis CP establece: «El que, con fines sexuales, determine a un menor de dieciséis años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de carácter sexual, aunque el autor no participe en ellos, será castigado con una pena de prisión de seis meses a dos años. Si le hubiera hecho presenciar abusos sexuales, aunque el autor no hubiera participado en ellos, se impondrá una pena de prisión de uno a tres años». Este tipo, que data de

la reforma operada al Código Penal en 2015, es heredero del antiguo delito de corrupción de menores y cumple la función de «recoger» aquellas conductas que no quedan comprendidas en los delitos de agresiones y abusos sexuales a menores pero que tienen virtualidad suficiente como para afectar de forma relevante al bien jurídico «indemnidad sexual».

Tras la reforma de 2015, se produce un cambio en la estructura de los delitos sexuales que afectan a menores de 16 años, y se pasa de la fórmula de describir la conducta como el ataque al bien jurídico, tal como sigue sucediendo en las agresiones y abusos sexuales a mayores (artículos 178 y 181 CP), para pasar a exigir que se verifique un contacto entre el autor y su víctima (art. 183.1 CP). De esta forma, el artículo 183 bis CP está preparado para responder en aquellos casos en los que no se produzca este contacto.

En el caso analizado, una menor de 7 años presencia cómo su avatar sufre una penetración simultánea por parte de dos varones. En nuestra opinión, esta conducta puede quedar subsumida en la expresión hacer «presenciar actos de carácter sexual, aunque el autor no participe en ellos». Al respecto, es oportuno recordar que el legislador, a efectos de su consideración como imágenes pornográficas, equipara «todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada», con lo cual queda clara la voluntad legislativa de considerar las imágenes y otras representaciones visuales como equivalentes a la realización de actos sexuales por parte de personas reales. Nada obsta tampoco a equiparar el visionado de actos que se desarrollen en presencia del menor con aquellos otros que tengan lugar a través de una pantalla. En este caso, además, se agrega el hecho de que la menor pueda considerar al avatar como una representación de sí misma y pueda vivir estos hechos como realizados sobre su persona (34) .

Lo cierto es que la última reforma operada al Código penal en materia de delitos sexuales que afectan a menores ha resultado especialmente confusa y ha creado tipos ambiguos que dan lugar a posibles solapamientos y concursos de leyes. En este sentido, entendemos que la conducta examinada también podría ser subsumida en el artículo 185 CP, que describe el exhibicionismo frente a menores de edad en los siguientes términos: «El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses». En este caso se trata de determinar si el hecho de manejar a un personaje virtual y hacerle realizar actos obscenos puede ser interpretado como la ejecución directa exigida por este tipo. Está claro que los sujetos que manejaron a los avatares no han hecho ejecutar actos obscenos a otra persona, por lo que no es posible hablar de la concurrencia de una autoría mediata, pero en nuestra opinión la ejecución directa puede abarcar la realizada utilizando los objetos materiales e inmateriales a los que se ha recurrido en este caso. En este sentido, es posible entender que quien maneja un ordenador y con él un personaje animado puede representar escenas obscenas y dar por cumplidos los elementos del tipo.

Cuestión distinta será la prueba de que el autor sabía que estaba efectuando esos actos frente a un menor de 16 años. Se trata de dificultades procesales que son comunes a los ciberdelitos y sobre las que nos referiremos en otro apartado. Nos obstante, en este supuesto la plataforma virtual en la que se desarrollan los hechos está destinada a juegos de niños de muy corta edad, lo que sugiere con claridad un conocimiento de las características de las víctimas. A favor de la aplicación del artículo 185 CP se suma también el hecho de que la pena prevista en este tipo —que consiste en la pena de prisión de seis meses a un año o multa de 12 a 24 meses— resulta más adecuada a la gravedad de la conducta que la prevista en el art. 183 bis (pena de prisión de seis meses a dos años).

La conducta narrada guarda cierta relación con los ataques que un grupo de hackers han llevado a cabo contra la compañía *Nintendo*. Estos sujetos han conseguido ejecutar juegos piratas en *Nintendo Switch*, e introducir imágenes pornográficas en el modo online de búsqueda de globos de *Super Mario Odyssey*. Nintendo es una compañía familiar y estos juegos están recomendados para niños de corta edad, lo que supone que un niño de 8 años puede encontrarse con una imagen pornográfica jugando a un juego de Mario (35) . En este caso debería entrar en escena el delito del artículo 186 CP, que establece que «el que, por cualquier medio directo, vendiere, difundiere o

exhibiere material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.» Al respecto, la expresión «por cualquier medio directo» podría poner en duda la aplicación de este tipo. Así, si se considera que sólo pueden quedar incluidas en el tipo las conductas en las que se exhibe el material de forma presencial al menor, el tipo no podría ser aplicado a la conducta expuesta. No obstante, entendemos que el visionado online de las imágenes también deber ser incluido en el tipo. En relación al elemento subjetivo, el conocimiento del sujeto de estar alterando un programa que es utilizado por niños supone, al menos, el dolo eventual respecto al visionado de las imágenes por parte de menores de edad.

Más allá de la concreta problemática de los ciberdelitos que es tratada en este trabajo, resulta oportuno señalar, una vez más, la necesidad de que se simplifiquen los tipos penales que castigan los ataques sexuales a menores en pro de la seguridad jurídica.

2. Prostitución y pornografía virtuales

En el juego los *Sims* en Línea se descubrió que un muchacho de 17 años, que actuaba bajo el nombre de «Evangeline», había construido un ciberburdel en el que empleaba a menores de edad y donde los clientes pagaban dinero virtual para tener unos minutos de cibersexo (36) . Como consecuencia de estos hechos, la cuenta del muchacho fue desactivada, pero no se entabló ninguna demanda judicial.

Incluso si las personas que manejaban los avatares de las prostitutas fuesen menores de edad, entendemos que este tipo de conducta no puede llegar a constituir un delito de prostitución. El delito de prostitución requiere que una persona se «prostituya». Si bien el legislador no aclara el contenido de este término, normalmente se considera por prostitución la prestación de servicios sexuales. Al respecto, no consideramos adecuado incluir dentro del concepto de prostitución la prestación de servicios que se realicen a distancia, como podría ser el caso de la atención telefónica de una línea erótica. De la misma manera no podrían quedar incluidos los servicios prestados por un personaje en un mundo virtual, ya que estos hechos no implican un contacto directo y no comprometen, por tanto, la integridad física de una persona.

Cuestión distinta será la posible valoración de estos sucesos como un delito del art. 189 CP si se han incluido imágenes que representen a menores. Este tipo castiga a quien «produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines». Al respecto, debemos recordar que el legislador en diversos apartados de la normativa se afana por aclarar que las imágenes reales y las simuladas deben ser equiparadas mientras estas últimas resulten ser «realistas».

Con el objeto de limitar las complicaciones que la excesiva amplitud del texto legal podía generar, la Circular 2/2015, de la Fiscalía General del Estado, dispone que solo se considerarán «imágenes realistas», potencialmente subsumibles en el concepto de pornografía infantil, aquéllas que se aproximen en alto grado a la representación gráfica de un auténtico menor, o de sus órganos sexuales, por lo que no se considerarán incluidos los dibujos animados, manga o representaciones similares, pues no serían propiamente «imágenes realistas», en tanto no perseguirían ese acercamiento a la realidad. A pesar de que la Fiscalía se esfuerza por limitar las posibles interpretaciones del texto legal, entendemos que no es posible excluir cualquier representación gráfica del contenido de este tipo, ya que de otra forma se derogaría el texto legal, que es muy claro en este sentido. En consecuencia, en aquellos casos en los que los dibujos sean suficientemente realistas no se podrá negar la aplicación del tipo (37) .

Respecto a esta problemática creemos oportuno señalar que existen determinados videojuegos que se acercan peligrosamente a la pornografía infantil. Es el caso del juego japonés «*Hizachi no naka no real*». Este entretenimiento consiste en tocar las zonas erógenas de una joven mientras se encuentra durmiendo, de forma que el jugador pierde si la chica se despierta. De la misma forma, el juego «*rapeplay*» es descrito como un simulador de violación. En este caso el objetivo consiste en violar a la mayor cantidad de mujeres posible, entre ellas una colegiala y una niña de diez años. El jugador lo podrá hacer en el metro, en un tren, en un parque y, si logra avanzar en

niveles, las debe obligar a abortar para luego convertirlas en sus esclavas sexuales. A mayor número de ataques y abusos virtuales, mejora el nivel del jugador.

En la cultura occidental también encontramos ejemplos de este tipo de juego. Es el caso de «*Rapeday*», en el que se controla a un sociópata durante un apocalipsis zombi y el juego consiste en acosa, matar y violar mujeres. En este juego el objetivo es la violación y no la supervivencia del personaje, a diferencia de lo que sucede en *Grand Theft Auto*, en el que el jugador puede tener sexo con una prostituta y luego matarla para recuperar el dinero (38) . A pesar de lo que podría pensarse en un primer momento, se trata de juegos que gozan de una notable aceptación entre aquellas personas que disfrutan de fantasías sexuales de violación (39) .

Nos encontramos ante hechos que discurren en una delgada línea entre el mal gusto y el delito. En estos casos, la concurrencia de un posible delito del artículo 189 CP deberá decidirse teniendo en cuenta el grado de realismo de las imágenes y situaciones que el juego plantea. Si bien es cierto que en el mundo de los videojuegos el asesinato, junto a otros muchos hechos socialmente reprobables, se encuentra totalmente normalizado, resulta difícil extender la misma valoración a conductas tales como la violación de un menor. No entraremos a valorar si este tipo de videojuegos tiene el efecto de perpetuar los estereotipos y apoyar la violencia contra las mujeres (40) . El efecto criminógeno de los videojuegos es un debate que se ha planteado en numerosas oportunidades. En este sentido, es un temor extendido el hecho de que los jóvenes que participan en juegos violentos confundan ficción con realidad y desarrollen un comportamiento criminal. No obstante, no existen evidencias científicas que demuestren esta relación (41) .

3. Robos y estafas virtuales

Como se ha señalado, la mayor parte de los juegos en línea dispone de su propia moneda. Estas monedas pueden ser intercambiadas y cuentan, por tanto, con un valor en el mundo real. Tal es el caso de *Linden Lab,* que dispone de los Dólares Linden. En el caso de los MMORPGS , los juegos no suelen contar con una moneda determinada; no obstante, se precisa de ciertos objetos, como oro o pociones mágicas, para hacer avanzar al personaje en la historia. Ya se ha indicado cómo a través de la agricultura del oro, la economía virtual se convirtió en una economía real. El hecho de que el dinero y los bienes virtuales gocen de un valor en el mundo real los convierte en posibles objetos materiales de delitos contra el patrimonio.

En la primera parte de este trabajo se explicó que resulta habitual que jugadores novatos se vean acosados por grupos de jugadores experimentados que exigen la entrega de bienes virtuales a cambio de permitirle continuar con su juego (42) . En estos casos no podremos hablar de un delito de robo, ya que los hechos no reúnen las características necesarias para estimar la concurrencia de los medios comisivos exigidos, esto es, la violencia y la intimidación. Si bien en estos casos existe efectivamente una amenaza condicional, que consiste en exigir la entrega del oro para poder continuar con el juego, ésta no reúne la entidad exigida en el delito robo con violencia o intimidación, donde el mal anunciado debe estar referido a la posibilidad de sufrir una daño de carácter personal y ser de producción inmediata.

Los ataques patrimoniales en el juego pueden darse utilizando otras modalidades. En 2003, en China un jugador se aprovechó de los agujeros de seguridad del juego Red Moon para apoderarse de la propiedad virtual de otro jugador. La víctima demandó a los creadores del juego y consiguió que los tribunales fallasen a su favor, de modo que la compañía se vio obligada a reponer los objetos virtuales (43) . Si bien el traslado de estos bienes no responde al concepto tradicional de «transferencia de activos», entendemos que esta conducta queda encuadrada en el artículo 248. 2. a), presentándose como una forma de estafa informática.

Por otro lado, el boom del juego *Pokémon* también multiplicó el número de estafas virtuales, ya que muchos jugadores que recurrieron a aplicaciones no oficiales del juego dejaron acceder a sus equipos sin saberlo a aplicaciones destinadas a obtener sus datos personales. Se trata de información —como contraseñas o números de cuentas bancarias— que permite a los criminales hacer transferencias de efectivo que en el momento de ser descubiertas resultan ya muy difíciles de ser rastreadas (44) . IZAGUIRRE OLMEDO también señala que la particular combinación entre el mundo real y el mundo virtual que ofrece este juego permitió que se cometieran otro tipo de ilícitos. El juego debía jugarse con el teléfono al aire libre, lo que provocó que se generaran

muchos falsos reportes de puntos o pokémons en zonas poco transitadas donde los delincuentes aprovechaban para robar los teléfonos a los usuarios (45) .

4. Acoso virtual

En los juegos MMORPGS, los participantes no compiten unos contra otros, no hay ganadores ni perdedores, se trata de ir haciendo avanzar al personaje a distintos niveles, lo cual puede llevar meses o años. Esto no significa que no se produzcan ataques entre los distintos avatares en situaciones concretas y que uno pueda matar a otro como parte del juego. En este sentido, es preciso distinguir los hechos que forman parte del desarrollo normal del juego de situaciones en las que se verifica el acoso sistemático de un participante. En estos casos se excede el margen de la diversión y se puede llegar a situaciones ilícitas.

El caso en el que se exige al jugador un beneficio económico para permitirle continuar con su juego es uno de estos supuestos, pero no es el único. No es preciso que se verifique una amenaza concreta para que crucemos esa línea. El artículo 172 ter recoge el delito de *stalking* en los siguientes términos: «1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana: 1.ª La vigile, la persiga o busque su cercanía física. 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas. 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella. 4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.»

Este delito contempla, por tanto, una situación de acoso sistemático. Elemento fundamental del tipo será que las conductas se repitan en el tiempo y como resultado lleguen a alterar el desarrollo de la vida cotidiana. La costumbre de participar en un juego puede formar parte de la vida de una persona, tal como puede suceder con otras muchas actividades. En este sentido, resulta habitual que quienes se involucran en los mundos virtuales hagan de ello una forma de vida y lleguen, incluso, a dedicar a este tipo de tareas más tiempo que al trabajo o al estudio. Por tanto, no parece descabellado suponer que el acoso que pueda afectar a las posibilidades de participar en un juego pueda suponer para una persona una verdadera alteración de su vida cotidiana (46) .

El delito del art. 172 ter CP exige también que este acoso se lleve a cabo a través de alguna de las conductas previstas en los incisos 1 al 4. Al respecto entendemos que nada obsta a que la vigilancia y persecución, o el establecimiento de un contacto puedan verificarse a través de un mundo virtual.

Como se ha señalado, el ciberespacio, y en concreto los mundos virtuales, son espacios de comunicación y de expansión de la personalidad que no pertenecen al mundo de la ficción, sino a una nueva realidad. De la misma forma que la comunicación puede llevarse a cabo a través de las redes sociales, puede verificarse en el mundo virtual creado para un juego.

En una línea similar de opinión, BRENNER propone la creación de un tipo delictivo que castigue la utilización de comunicaciones originadas por medio de un ordenador para infringir maliciosamente angustia emocional a alguien (47) . En nuestra opinión, a la conducta ideada por esta autora debería añadirse el elemento de la reiteración para que podamos estar en el ámbito del acoso y se pueda llegar a la gravedad suficiente como para exigir la intervención de las normas penales. Esta circunstancia seguiría dejando fuera de la valoración de las normas penales al caso del payaso violador.

Un tipo de acoso que se ha convertido en algo normal en estos mundos es el que sufren los agricultores del oro. Se trata de personajes que son muy mal vistos por los jugadores ya que, en su opinión, pervierten el normal desarrollo del juego. El hecho de que circule gran cantidad de oro y de objetos mágicos en el mercado negro ha generado la inflación de estos valores virtuales (48) . Al haber mucho oro disponible, éste tiene menos valor. Además, estos personajes son fácilmente reconocibles en el mundo virtual porque que sus movimientos son muy repetitivos: se dedican una y otra vez a la realización de tareas muy sencillas para conseguir unas pocas monedas. Esta

situación ha dado lugar a que circulen por la web mensajes del tipo «muerte a los agricultores chinos», que generan un acoso sistemático en la web por parte de determinados jugadores (49) . El hecho de morir una y otra vez y tener que perder un valioso tiempo en resucitar al personaje puede llevar a estos trabajadores a ver afectado el rendimiento de su trabajo (50) .

En los últimos tiempos muchos medios de comunicación se han hecho eco del acoso que sufren muchas jugadoras en los mundos virtuales por el mero hecho de ser mujer. Hubo una época en la que la industria del videojuego estaba enfocada prácticamente a los hombres. Ahora el panorama está cambiando. Según la Asociación Española de Videojuegos (AEVI), durante el 2015 había 15 millones de usuarios en España. Un 47% eran mujeres (51) . Muchas de ellas han sido víctimas de comportamientos impropios que pueden ir desde comentarios sexistas hasta un verdadero boicot para que abandonen el juego a través de desprestigio, humillación, persecución, intentos de *phishing,* o extorsión (52) .

Pero el sexismo no es la única razón que da lugar a situaciones de acoso en los mundos virtuales. En ocasiones, los jugadores con personajes más violentos y más avanzados hacen *bullying* a oponentes más débiles para sentirse más poderosos sobre los demás. Incluso esos acosadores llegan a coordinarse para acosar a otro jugador por cualquier motivo, ya sea dentro del mundo del juego o a través de mensajes; en los casos más extremos, se llega al acoso fuera del juego (53) .

La compañía *Blizzard* ha introducido en el Reino Unido, en su famoso juego *Overwatch,* un nuevo sistema para reportar jugadores. Este sistema va enfocado, precisamente, a luchar contra esas amenazas. El sistema permite reportar a gente por trato abusivo, trucos, «*griefing*» (enojar, molestar o impactar negativamente la experiencia de juego de otro jugador) o mal trabajo en equipo, entre otras opciones. Cada uno de los motivos lleva una explicación sobres sus usos adecuados. En este sentido, el chat abusivo se refiere a cualquier comentario de odio, discriminatorio u obsceno (54) . A diferencia de la mayoría de juegos, *Overwatch* ha puesto sobre la mesa las herramientas para denunciar y limpiar la comunidad de su juego; no obstante, no puede dejarse de lado el hecho de que los casos más extremos de acoso deben recibir también una respuesta penal.

5. ¿Delitos contra la ética en el juego?

En el año 2018, Corea del Sur se ha convertido en el primer país en aprobar la criminalización del «*boosting*», o «nivelación de potencia». Como se ha explicado, la nivelación de potencia consiste en jugar con cuentas ajenas y subirles de nivel o de rango competitivo debido a que el jugador oficial no posee habilidades necesarias para hacerlo de manera independiente. Estos servicios de «*boosting*» se contratan a jugadores de alto nivel por un precio elevado y, especialmente en Corea del Sur, se han convertido en práctica constante en videojuegos como *Overwatch* y *League of Legends*. La enmienda que introduce esta medida fue acuñada a la Ley de Promoción de la Industria de Videojuegos tras meses de debate de la Asamblea Nacional de Corea, en compañía de desarrolladoras de videojuegos como *Blizzard* y *Riot Games*. Las penas por esta infracción serán de dos años de prisión y una multa de 18 mil dólares. Situada entre las regiones clave de la industria, en Corea del Sur los videojuegos ingresan unos 50 millones de dólares al año y se estima que alcanzarán los 1.500 millones en 2020 (55) . En el país asiático, los grandes jugadores profesionales de videojuegos son figuras de televisión y suelen ser modelos a seguir en la cultura surcoreana, por lo que muchos de los jóvenes contratan a los *boosters* para aumentar su ranking y ser mejor vistos en sociedad. Esta práctica podría implicar, por tanto, una deslealtad en una competencia deportiva y suponer la atribución de unos méritos no obtenidos limpiamente.

En el Código penal español la figura que resulta más cercana a la recientemente introducida en la legislación surcoreana es el delito de corrupción en el deporte, que se tipifica en el art. 186 bis 4 CP como una forma de corrupción en el sector privado. La reforma introducida al Código Penal en 2015 modificó este precepto, indicando que esta normativa resultará aplicable al fraude en cualquier «encuentro o competición deportiva de especial relevancia económica o deportiva», añadiendo, además, que «se considerará competición deportiva de especial relevancia económica, aquélla en la que la mayor parte de los participantes en la misma perciban cualquier tipo de retribución, compensación o ingreso económico por su participación en la actividad; y competición

deportiva de especial relevancia deportiva, la que sea calificada en el calendario deportivo anual aprobado por la federación deportiva correspondiente como competición oficial de la máxima categoría de la modalidad, especialidad, o disciplina de que se trate» (56) .

Ello nos lleva a plantear si la participación en una competición de videojuegos online puede quedar comprendida en este tipo. Al respecto, es conveniente recordar que, tal como sucede en el resto de los deportes, la mayor parte de las competiciones quedarán excluidas por no reunir los requisitos de relevancia exigidos en el tipo. En consecuencia, el precepto español dista notablemente de la legislación surcoreana que pretende castigar el *boosting* como actividad genérica. En el ámbito de los mundos virtuales multijugador se deberá añadir, además, que muchos de estos juegos no podrán ser considerados como encuentros o competiciones deportivas, ya que no suele tratarse de competiciones donde los jugadores se enfrenten unos con otros por vencer en el juego. El desarrollo de los personajes en muchos de los mundos virtuales suele ser independiente y cada uno de ellos intentará avanzar en el juego de forma individual.

No obstante, el fraude en los grandes campeonatos de videojuegos en ocasiones sí podrá dar lugar a la aplicación del delito comprendido en el artículo 286 bis 4 CP. En este sentido, es posible sostener que las competiciones de videojuegos online pueden llegar a reunir las características exigidas por el tipo, ya que en nuestro país se celebran importantes competiciones profesionales que están organizadas por la Liga de Videojuegos Profesional (LVP). Actualmente, esta Federación organiza campeonatos profesionales y amateur y cuenta con importantes patrocinadores (57) .

A nuestro criterio, la principal polémica que plantean estos delitos se refiere a la conveniencia de que el Derecho penal castigue conductas que sólo afecten a la ética en el deporte. Aunque el *boosting* pueda ser visto como una forma de corrupción, la corrupción no es más que una forma de atacar bienes jurídicos (58) . En consecuencia, como a través de un constreñimiento físico se puede lesionar la libertad sexual, utilizando el abuso de un poder de decisión se puede dañar la función pública o el patrimonio. Ello conduce a que los actos de corrupción no merezcan un castigo en sí mismos si no es en relación a los bienes jurídicos cuya lesión o puesta en peligro provocan. En nuestra opinión, el deporte es una actividad privada donde no es posible hallar un bien jurídico a proteger más allá del patrimonio. Desde nuestro punto de vista, no existe ningún bien jurídico referido a la «lealtad deportiva» que pueda merecer protección penal. A pesar de ello, el legislador español parece manifestarse en contra de esta postura al incluir en el art. 286 bis 4 CP no sólo a las competiciones que resultan relevantes desde un punto de vista económico, sino también aquellas que son importantes únicamente desde el punto de vista deportivo (59) .

6. Blanqueo de capitales

Si la creación de medios electrónicos de pago ya supuso una enorme dificultad para el control de las operaciones económicas (60) , la creación de monedas virtuales ha incrementado mucho más el riesgo del lavado de dinero. Los mundos virtuales brindan la oportunidad de mover grandes cantidades de dinero a través de las fronteras, sin restricciones y con un riesgo mínimo de ser detectados.

Inicialmente los jugadores sólo podían convertir la moneda virtual a real a través del uso de sitios de subastas en línea. Esto cambió para permitir a los jugadores convertir sus ingresos digitales en moneda real directamente mediante el uso de sitios web de comercio de moneda virtual. La convergencia con el mundo real se acercó un paso más cuando *Entropia Universe* (61) introdujo al mundo real tarjetas de cajeros automáticos a sus jugadores para permitirles retirar de forma instantánea dinero en efectivo de su mundo virtual (62) .

Pronto se detectó que *Second Life* se podría utilizar para el lavado de dinero. Para ello, un jugador puede usar su tarjeta de crédito o débito real para comprar dinero en línea. Luego debería canjear esos créditos por dinero real con otro jugador en otro país y utilizar la unidad monetaria de ese país. Resulta muy sencillo en la medida en que para crear una cuenta en *Second Life* sólo es necesario proporcionar un nombre y una dirección de correo electrónico y no hay ninguna verificación de esa información. A su vez, para realizar la compra de los dólares Linden se puede utilizar una tarjeta de crédito o una cuenta de *Pay Pal.* Aquí es donde podría haber algún tipo de seguimiento; sin embargo, si se utilizó información ficticia para establecer las cuentas, la investigación se encontrará pronto en un callejón sin salida (63) .

La FAT (Panel Asesor de Fraudes de Gran Bretaña) es un organismo de control establecido por el Instituto de Contadores Públicos en Inglaterra y Gales y ha hecho público un informe en el que pide al Gobierno que extienda la regulación financiera del mundo real a *Second Life* y juegos similares. Este organismo sostiene que las bandas criminales o terroristas pueden usar el juego para mover fondos y evitar la vigilancia. Para remarcar la importancia del capital que se maneja en estos juegos, es pertinente señalar que en 2006 Ailin Graef, un maestro nacido en China que vive en Alemania, afirmó haberse convertido en la primera persona en ganar $ 1 millón de dólares en *Second Life*. Su «avatar», Anshe Chung, amasó la fortuna al desarrollar propiedades virtuales y venderlas o alquilarlas a otros «avatares» (64) .

Lo cierto es que *Second Life* vivió sus momentos de esplendor en los años 2006 y 2007 y a partir de 2010 comenzó a bajar el número de cuentas activas. A día de hoy el mayor peligro de la utilización de los mundos virtuales para el lavado de dinero se centra en los juegos online. En consecuencia, la doctrina ha analizado los pasos que resultarían necesarios para conseguir blanquear activos utilizando los MMORPGS. Así, entre otras opciones se ha detallado que el blanqueo podría desarrollarse de la siguiente forma (65) :

a) Adquirir un número de tarjeta de crédito robado.

b) Crear una nueva cuenta con una tarjeta prepago en un MMOG con un mercado activo de cultivo de oro, que permita tanto la compra como la venta de la moneda del juego. Resulta fundamental que los bienes virtuales se puedan comprar y vender.

c) Ir a los sitios web de cultivo de oro y comprar dinero con la tarjeta robada y transferirlo a la nueva cuenta

d) Iniciar sesión con una segunda cuenta que haya sido comprada con una tarjeta de crédito o tarjeta de regalo prepago diferentes, para que ambas cuentas se registren al mismo tiempo.

e) Transferir el dinero de la primera cuenta a la segunda y borrar luego la primera cuenta.

f) Finalmente, vender el dinero en un lugar diferente a aquel en el que se compró y transferir los ingresos a una nueva cuenta bancaria.

Durante el último año, el juego que ha visto incrementada su popularidad ha sido *Fornite*. *Epic Games*, la compañía creadora, ha ganado sólo en 2018 alrededor de 2,6 millones de euros con compras que se realizan dentro del juego. *Fortnite* utiliza una divisa virtual y única llamada paVos (*V-bucks* en inglés), que se puede obtener comprando tarjetas con códigos que se canjean dentro del juego o realizando pagos por Internet con tarjetas de débito y/o crédito. Así, un sujeto puede crearse una nueva cuenta gratuita para *Fortnite* y gracias a una tarjeta de crédito robada puede empezar a gastar dinero real para adquirir la moneda usada en el juego, aumentando el valor de la cuenta con créditos *V-Buck* y también «*skins*» (ítems) y todo lo que se pueda adquirir dentro de la tienda del juego . Cuando ya tiene una cuenta con un valor económico relevante, la vende por una cantidad mínima de su coste real. Si, por ejemplo, el cibercriminal ha acumulado *V-Bucks y skins* por valor de 100 euros, la cuenta la venderá en plataformas como *eBay* o *G2G* por 25€. Y normalmente usando como medio de pago una transferencia bancaria por servicios como *Paypal*. Una vez la cuenta ha cambiado de manos, también lo hace el email y contraseña usadas en la cuenta vendida. De esta manera, aunque se haya dejado 75€ en el proceso, el criminal ha blanqueado 100€ robados en 25€ de moneda legal. Si esta operación se multiplica utilizando diversas cuentas y tarjetas robadas es posible blanquear sumas elevadas de dinero (66) . Sin embargo, los precios más atractivos se pueden encontrar en la *deep web*, donde el mercado es mucho más pujante dada la naturaleza de esta parte oculta de Internet (67) .

Además, hay que tener en cuenta que, si el sujeto realiza la transacción usando criptomonedas, entonces seguir el rastro de la operación será una tarea casi imposible. Resulta evidente que, cuanto más dinero se mueva a través de los canales bancarios, los gobiernos tendrán más posibilidades de ejercer el control y prevenir el fraude y el blanqueo de dinero. No puede negarse que los ciudadanos pretendan preservar el anonimato y la confidencialidad de su actividad económica y ello no necesariamente ocurrirá fuera de la legalidad (68) , pero si creará más oportunidades para el delito.

VI. Las dificultades en la investigación de los delitos virtuales

La persecución y castigo de los ciberdelitos se ve entorpecida por una serie de dificultades técnicas y procesales:

1. La determinación del autor de los hechos

A la hora de investigar la autoría de los ciberdelitos, los proveedores de servicio de Internet prestan una información determinante, ya que, para localizar el ordenador desde el que se ha cometido un determinado delito, el primer paso consiste en averiguar la dirección IP. Al respecto, es pertinente aclarar que no todos los usuarios tienen su propia dirección IP. Las empresas a las que se les contrata el servicio de internet y que administran las cuentas tienen más clientes que direcciones para asignar, dado que el número de estas direcciones es finito. De tal forma, las compañías tienen que repartir lo mejor posible los recursos. Es una realidad que siempre hay un porcentaje de clientes que están desconectados, por lo que las direcciones disponibles se van asignando entre los usuarios a medida que éstos las requieren y, cuando una persona apaga su conexión, esa IP que ha quedado disponible pasa a ser utilizada por otra persona. Este sistema es conocido como dirección dinámica. Por otro lado, la conexión estática es aquella que es utilizada por las páginas webs y por ciertos usuarios que escogen la opción de pagar más para poder contar con una dirección IP propia (69) . Así, para poder saber quién ha sido el autor de un ciberdelito, no sólo se debe averiguar la dirección IP del terminal desde el que se ha realizado la conducta, sino también la fecha y la hora de la comisión.

En consecuencia, para evitar ser descubierto por la comisión de un delito, lo primero es intentar ocultar la IP del aparato desde el que se ha cometido. Para ello existen distintas estrategias. La primera de ellas consiste en acudir a un cibercentro y utilizar una de sus terminales. También existe la posibilidad de acudir con el propio equipo a un cibercafé desde el que se pueda utilizar la conexión a internet. Finalmente, si se desea hacer uso de una conexión propia, también se plantea la posibilidad de utilizar los programas llamados «proxys» (que podemos traducir como «representantes»). Un proxy es una máquina situada entre nuestro ordenador y el destino. Para solicitar una web, nuestro ordenador envía un paquete con su propia dirección a la web de destino. Al utilizar un proxy, en lugar de solicitar la web de forma directa, nuestro ordenador contacta con otra que recibe el encargo y lo canaliza al servidor de la web solicitada. De esta manera, en el servidor de la web solicitada quedará almacenada la IP del intermediario en lugar de la nuestra.

La red oscura funciona de forma similar a los proxys. Así, la herramienta más utilizada para navegar en la *dark web* es la denominada TOR. Estas siglas vienen, precisamente, de la expresión *The Onion Router*, es decir, el encaminamiento cebolla. Se trata de un símil sobre la forma en la que se va protegiendo la identidad real del que usa la web (70) . A pesar de estas opciones, ningún método otorga la completa seguridad de no ser localizado.

Cada año, el Centro Europeo de Ciberdelincuencia (EC3) de Europol publica su evaluación sobre la amenaza de la delincuencia organizada en Internet (IOCTA, por sus siglas en inglés). Se trata de un informe estratégico y emblemático sobre hallazgos clave, amenazas emergentes y desarrollos de la ciberdelincuencia. El Informe publicado en 2018 pone de manifiesto que 2017 fue un año particularmente tumultuoso para los mercados de la web oscura, ya que tres de los mercados más grandes, *Alpha Bay, Hansa* y *RAMP,* fueron eliminados gracias a la aplicación de la ley internacional. Para poner de manifiesto el volumen de negocios al que nos referimos conviene agregar que *AlphaBay* llegó a albergar a más de 200.000 usuarios y 40.000 proveedores. Así, hubo más de 250.000 listados de drogas ilegales y sustancias químicas tóxicas en *AlphaBay* y más de 100.000 listados de documentos de identificación robados y fraudulentos, productos falsificados, malware y otras herramientas de piratería informática, armas de fuego y servicios fraudulentos. Se estimó de manera conservadora que el sitio ha tenido que pasar USD 1.000 millones a través de sus libros de contabilidad desde que abrió sus puertas en 2014 (71) .

Volviendo a los pasos de la investigación para poder llegar al autor del delito, es conveniente indicar que la identificación de la terminal desde la cual se ha cometido el crimen no soluciona por completo el problema de la determinación de la autoría, ya que, realizando la investigación sobre los datos de tráfico, se podrá identificar al equipo y a la persona abonada, pero siempre existe la

opción de que la conexión a internet haya sido utilizada por un tercero con fines delictivos (72) . Resulta fácil que ello suceda cuando no se conocen los peligros de internet y no se toman las medidas de seguridad necesarias para evitarlo, como, por ejemplo, estableciendo una contraseña para poder acceder a la red. Esta posibilidad obligará a las Fuerzas de Seguridad a utilizar en la investigación de este tipo de ilícitos no sólo métodos tecnológicos, sino también métodos tradicionales. Se trata de la clásica vigilancia policial apoyada en procedimientos comunes, como la vigilancia personal o las intervenciones telefónicas, entre otras opciones (73) .

2. El uso de monedas virtuales

El Parlamento Europeo ha prestado atención al fenómeno de las criptomonedas, mereciendo ser destacada la Resolución de 26 de mayo de 2016, en la que se pone de manifiesto que las monedas virtuales pueden contribuir positivamente al bienestar de los ciudadanos y al desarrollo económico.

Así, entre otros posibles beneficios, se destaca que estas monedas pueden reducir los costes de las operaciones y los costes de funcionamiento de los pagos y, en particular, de las transferencias transfronterizas. Por otro lado, esta Resolución también llama la atención sobre los posibles riesgos debido a las posibilidades de realizar operaciones en el mercado negro, blanqueo de dinero, financiación del terrorismo, fraude y evasión fiscal y otras actividades delictivas basadas en la «pseudonimia» y la «combinación de servicios» que ofrecen algunos de estos servicios y la naturaleza descentralizada de algunas monedas virtuales, habida cuenta de que la trazabilidad de las operaciones en efectivo tiende a ser muy inferior (74) .

Siguiendo esta línea, se ha sostenido que el valor de una criptomoneda es secundario en relación a sus otros atributos. La diferencia fundamental con el dinero tradicional es la ausencia de una autoridad central que controle las transacciones que se realizan, pero, a cambio, otra de sus características definitorias es la volatilidad, ya que están sujetas a ataques financieros, fluctuaciones y a la pérdida de confianza de los usuarios (75) . Otro de sus puntos fuertes es indudablemente el anonimato. Por tanto, las criptomonedas son el principal mecanismo para el pago de servicios criminales de una gran cantidad de productos situados en la web oscura. A día de hoy *Bitcoin* sigue siendo la criptomoneda más utilizada en la ciberdelincuencia.

Históricamente, Bitcoin disfrutó de más del 80% de la cuota de mercado de la criptomoneda, pero a principios de 2017 este porcentaje se había reducido a menos del 35%. Sin embargo, esto no se refleja en las investigaciones de delitos cibernéticos en la Unión Europea, donde *Bitcoin* sigue siendo la criptomoneda más frecuente. Dicho esto, algunos Estados Miembros destacan un pequeño cambio hacia monedas más orientadas a la privacidad, como *Monero* o *Zcash* (76) . Si bien la naturaleza descentralizada y desregulada del *blockhaim* (cadena de bloques) (77) , gracias al cual funciona *Bitcoin*, la hace ideal para ser utilizada en actividades delictivas, no es totalmente resistente a las actividades de rastreo. Por esta razón ha nacido el interés en buscar criptomonedas alternativas que cuenten con características mejoradas de anonimato y privacidad (78) .

Al respecto, el Informe del Centro Europeo de Ciberdelincuencia de 2018 señala que los agentes intercambiadores de criptomonedas hasta entonces eran considerados como potenciales pistas de investigación, ya que representaban nexos en los que los fondos criptográficos criminales cruzaban el sistema financiero regulado. No obstante, esta línea de investigación ha dejado de ser prioritaria, ya que estos servicios han evolucionado con el surgimiento de lo que se conoce como «*swappers*». Se trata de intercambios semiautomáticos que no requieren ningún procedimiento en el que se conozca la identidad del cliente. Estos intercambios permiten a los usuarios intercambiar una criptomoneda no solo a monedas fiduciarias, sino también realizar intercambios entre diferentes criptomonedas. Por otro lado, también ha tenido lugar la llegada de intercambios descentralizados, que permiten intercambios de igual a igual y tampoco requieren el uso de métodos de identificación de clientes.

Las monedas virtuales carecen actualmente de una regulación legal específica, manteniéndose en el ámbito de lo permitido, pero no regulado (79) . El Parlamento Europeo, en su Resolución de 26 de mayo de 2016, ha indicado que, para abordar los riesgos generados por las monedas virtuales, será necesario aumentar la capacidad reguladora, incluidos los conocimientos técnicos, así como desarrollar un marco jurídico sólido que esté a la altura de la innovación, garantizando una respuesta oportuna y proporcionada. No obstante, también ha advertido que, si se adopta una

regulación de manera precoz, ésta podría no estar adaptada a una realidad todavía en evolución y transmitir a la población un mensaje erróneo sobre las ventajas o la seguridad de las monedas virtuales (80) .

Por el momento, la Directiva (UE) 2018/843, del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (81) , ha introducido ciertas referencias en esta materia. Así, ha remarcado el peligro que representa el hecho de que los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como los proveedores de servicios de custodia de monederos electrónicos, no estén obligados por la Unión a detectar actividades sospechosas, razón por la que resulta esencial ampliar el ámbito de aplicación de la Directiva (UE) 2015/849 para incluir en él a los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias, así como a los proveedores de servicios de custodia de monederos electrónicos. A los efectos de la lucha contra el blanqueo de capitales y la financiación del terrorismo, las autoridades competentes deben estar facultadas, a través de las entidades obligadas, para vigilar el uso de las monedas virtuales (82) .

A pesar de estas medidas, el anonimato de las monedas virtuales permite su posible uso indebido con fines delictivos. Por ello, la Directiva resalta que la inclusión de los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y de los proveedores de servicios de custodia de monederos electrónicos no resolverá totalmente la cuestión del anonimato asociado a las transacciones con monedas virtuales, al mantenerse el anonimato en gran parte del entorno de la moneda virtual, puesto que los usuarios pueden llevar a cabo transacciones al margen de tales proveedores de servicios. En consecuencia, la Directiva señala que, para combatir los riesgos relacionados con ese anonimato, las Unidades de Inteligencia Financiera (UIF) nacionales deben poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual. Además, debe analizarse más a fondo la posibilidad de que los usuarios efectúen, con carácter voluntario, una autodeclaración a las autoridades designadas.

3. El carácter transnacional de los delitos

La red ha eliminado las fronteras al permitir que se establezcan comunicaciones e interacciones instantáneas entre personas que se encuentran en distintos puntos del planeta. Esta expansión del ámbito comunicativo implica, a su vez, la multiplicación de la potencialidad lesiva de una *conducta delicti*va en comparación con lo que ocurriría en el espacio físico. Así, la contracción del espacio y la interconexión de los sistemas dan como resultado un crecimiento exponencial de los efectos de un delito (83) .

Por otro lado, el gran beneficio que implica la eliminación de las fronteras de la comunicación tiene también el evidente inconveniente de que se pueda realizar una *conducta delicti*va en un país, mientras que sus efectos tienen lugar en otro diferente. Mientras Internet es un espacio sin fronteras, las leyes y, por tanto, la investigación de los cibercrímenes se encuentran confinadas a los límites impuestos por la soberanía de los Estados. Esta circunstancia lleva a la necesidad de unificar criterios legales y estrechar la colaboración en la persecución y castigo de este tipo de ilícitos (84) .

En el ámbito europeo, el documento de referencia es el Convenio de Budapest sobre Ciberdelincuencia, que fue puesto a consideración de los Estados Miembros el 23 de noviembre de 2001 por el Consejo de Europa. Este convenio tiene la particularidad de que fue abierto a la firma de cualquier país del mundo, opción que fue celebrada por la doctrina, que la ha calificado como «acertada» al tener en cuenta que el problema de la cibercriminalidad se resiste a ser enmarcada en límites territoriales (85) . El Convenio persigue un triple objetivo (86) :

— Establecer una tipificación común de ciertas infracciones penales, posibilitando de este modo la armonización de la legislación pertinente a nivel nacional.

— Establecer unas facultades y técnicas comunes de investigación mejor adaptadas al medio de las tecnologías de la información, posibilitando de este modo la armonización de las normas procesales penales de los diferentes países.

— Establecer nuevas y adaptar antiguas formas de cooperación internacional, posibilitando de este modo que los Estados actúen de concierto en la aplicación de las facultades y poderes de investigación y persecución que contempla el Convenio, por ejemplo, mediante la utilización de una red de contactos permanentes.

En relación a los mecanismos desarrollados para la lucha y prevención de estos delitos destaca la creación, en 2013, por parte de Europol, del Centro Europeo de Ciberdelincuencia. Su estrategia y mecanismo de prevención se basa en el Proyecto 2020, fundamentado en la Alianza Internacional de Protección para la Ciberseguridad (denominado ICSPA, por las siglas en inglés: «*International Cyber Security Protection Alliance*»). Se trata de un estudio dirigido por la Europol , que tiene como objeto adelantar la visión gubernativa y de las fuerzas oficiales a las posibles consecuencias que, en materia penal y criminal, pudieran resultar del avance de las nuevas tecnologías (87) .

4. Las organizaciones virtuales transnacionales

Cada vez en mayor medida los ciberdelitos no son el resultado de actuaciones individuales, sino que son realizados por organizaciones de carácter trasnacional. El conocimiento por parte de unos pocos de una vulnerabilidad del sistema que se quiere explotar suele ser el punto de partida. De ahí en más, estos sujetos se encargarán de organizar la trama y de repartir los papeles. Por tanto, varias personas suelen intervenir de común acuerdo según la especialidad de sus conocimientos o de acuerdo a la función que desempeñan dentro de la organización criminal con un objetivo común. Suele ser habitual que los distintos miembros del grupo no conozcan la identidad de los demás, o bien que sólo conozcan el seudónimo que utilizan en la red. Para comunicarse entre sí los miembros de la organización pueden recurrir a métodos seguros de la *deep web*. Así, utilizando el programa TOR podrán utilizar el TOR Mail o bien el TORChat y comunicarse en tiempo real (88) .

Este tipo de organización suele estar formada por distintos eslabones o subgrupos que tienen asignadas tareas específicas. Ejemplificando esta situación, se puede indicar que en una organización destinada a efectuar estafas cibernéticas, además de los organizadores, podrán encontrarse los programadores, que serán ingenieros expertos capaces de escribir el código informático para explotar el error, los distribuidores masivos, que se encargarán de obtener listas de correos electrónicos o cuentas de whatsapp y de enviar mensajes, otro grupo encargado de gestionar los cobros y de asegurarse de que el rastro del dinero no pueda ser seguido, y un grupo de muleros, esto es, individuos reclutados para recibir los envíos de dinero. Evidentemente, no todas las organizaciones contarán con todos los grupos, y es posible también que algunos sujetos desarrollen distintas funciones, dependiendo de las características de los ciberdelitos que se cometan (89) . Una característica que suele encontrarse en la mayor parte de los casos es que se trata de organizaciones con una estructura horizontal, casi difusa, donde los miembros actúan conjuntamente pero con cierta independencia (90) .

Lógicamente, este tipo de trama delictiva dificultará la determinación del grado de participación de cada sujeto en el delito, y particularmente la atribución de la autoría a los organizadores que no han participado directamente en el hecho y que no han tenido el dominio específico de la ejecución de la acción (91) .

VII. Conclusiones

Existe una anomia generalizada en el ciberespacio, por lo que el usuario infractor vive en la creencia de que se encuentra en un espacio ajeno al Derecho (92) . Por ello, es preciso que el Derecho se plantee cómo puede actuar para garantizar a los ciudadanos en los mundos virtuales el disfrute de los derechos y libertades individuales al mismo nivel que en el universo físico (93) . Tal como plantea MIRÓ LLINARES, si bien hoy en día la incidencia de la ciberdelincuencia puede ser testimonial, conforme vaya avanzando la tecnología y ésta invada cada vez en mayor medida nuestra vida diaria, el número de delitos cometidos a través de internet se verá incrementado (94) . En particular, en referencia al objeto de nuestro trabajo, no parece descabellado suponer que el uso de los mundos virtuales se irá expandiendo y alcanzando otros ámbitos de actuación.

Resaltando las dificultades en la persecución de este tipo de delitos, RAYÓN BALLESTEROS y

GÓMEZ HERNÁNDEZ han sostenido que «sería deseable que las nuevas legislaciones modernas puedan hacer frente a las múltiples manifestaciones de la ciberdelincuencia mediante la configuración de tipos penales abiertos, dejando al margen casuísticas descriptivas, complejas y farragosas. En su opinión, lo más adecuado sería realizar una reelaboración de las categorías fundamentales del Derecho y del procedimiento penal, sobre los cuales se sustenta la responsabilidad criminal, para establecer tipos penales abiertos que pudieran contener los requisitos para la persecución de conductas dañosas y perjudiciales para la sociedad cualquiera que sea el estado de desarrollo de la tecnología» (95) .

Entendemos que no es posible descartar que en un futuro se requiera una legislación más especializada para atender a las situaciones conflictivas que se den en estos entornos. No obstante, lo cierto es que, a día de hoy, el Derecho penal cuenta con instrumentos suficientes como para enfrentarse a las situaciones que se plantean. Lo relevante, bajo nuestro criterio, será que la existencia de estos mundos virtuales no funcione como una barrera de contención del Derecho. Internet no puede seguir siendo el mundo sin reglas. No todo vale en un mundo virtual.

Se ha sostenido que existe una importante cifra negra en materia de cibercriminalidad (96) . No cabe duda de que una de las principales razones que llevan a que un ciudadano no denuncie un delito cometido en internet es la generalizada sensación de que en este ámbito existe una impunidad absoluta, situación que se ve incrementada si nos referimos al mundo virtual de los juegos. Creemos que éste es el ámbito en el que se debe incidir, concienciando a los usuarios de internet de que no se encuentran desprotegidos por haber traspasado las fronteras de un mundo virtual.

Notas

(1) El presente trabajo ha sido elaborado en el marco del Proyecto I+D+i, del Programa Estatal de Investigación, Desarrollo e Innovación orientada a los retos de la sociedad, DER2017-85612-R «Ciberataques y Gobernanza Global», del Ministerio de Ciencia, Innovación y Universidades.

Ver Texto

(2) DIBBELL, J.: «Una violación en el ciberespacio. Cómo un payaso malvado, un espíritu engañoso haitiano, dos magos y un elenco de docenas convirtieron una base de datos en una sociedad», publicada por primera vez en *The Village Voice*, 23 de diciembre de 1993. Disponible en: http://www.juliandibbell.com/texts/bungle_vv.html (visto el 26/06/2019).

Ver Texto

(3) *Roblox* es una plataforma de videojuegos destinada a menores de edad donde los usuarios no solo pueden participar en los juegos, sino también crear sus propios universos virtuales y ponerlos a disposición de la comunidad de internautas. RODELLA, F.: «Polémica por la violación del avatar de una niña de siete años en un popular videojuego. Roblox, plataforma donde los usuarios pueden crear sus propios universos virtuales para jugar online, ha borrado el juego al que accedió la pequeña tras la denuncia de la madre», en *El País*, 6 de julio de 2018, disponible en: https://elpais.com/tecnologia/2018/07/06/actualidad/1530871736_133106.html (visto el 26/06/2019).

Ver Texto

(4) Casas Herrer explica que las líneas telefónicas tradicionales sobre las que trabajaban los módems de fin de siglo carecían de la capacidad suficiente para intercambiar la ingente cantidad de datos que requerían los juegos en línea; por esta razón nacieron los cibercentros, donde las partidas se realizaban utilizando una conexión rápida que era prohibitiva para un particular. De esta forma, el mundo del juego duraba, en aquellos años, sólo el tiempo que tardaba en trascurrir una partida. CASAS HERRER, E.: *La red Oscura. En las sombras de internet. El cibermiedo y la persecución de los delitos tecnológicos*, Madrid, 2016, pág. 202.

Ver Texto

(5) Disponible en https://uo.com/what-is-uo/ (visto el 27-06-2019).

Ver Texto

(6) IRWIN, A. S. M. y SLAY, J.: «Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft», en *Edith Cowan University Research Online*, 2010. Disponible en https://www.researchgate.net/publication/49285565_Detecting_Money_Laundering_and_Terrorism_Financing_Activity_in_Second_Life_and_World_of_Warcraft (visto 26/06/2019), pág. 42.

Ver Texto

(7) CHECA GARCÍA, F.: «El uso de metaversos en el mundo educativo: gestionando conocimiento en Second Life», en *Revista de Docencia Universitaria*, vol. 8, nº 2, pág. 149.

Ver Texto

(8) CASAS HERRER, E.: *La red Oscura…,* ob. cit., pág. 205.

Ver Texto

(9) PÉREZ ROMERO, G.: *Second Life. Nuevos comportamientos artísticos a través de los espacios expositivos de la realidad virtual*, Tesis Doctoral . Universidad de Granada, disponible en: http://digibug.ugr.es/handle/10481/44062 (visto 18-7-2019), pág. 43.

Ver Texto

(10) PÉREZ ROMERO, G.: *Second Life*…, ob. cit., pág. 14.

Ver Texto

(11) LUNA, J. A.: «El mundo de 'Second Life' resucita gracias a la realidad virtual», en *El Diario.es*, 18 de enero de 2017, disponible en: https://www.eldiario.es/tecnologia/Second-Life-resucita-gracias-realidad_0_671233050.html (visto 17-7-2019).

Ver Texto

(12) *War of Warcraft* es un juego producido en Irvine, California, por *Blizzard Entertainment*. Es uno de los juegos de computadora más rentables de la historia, que ha llegado a producir mil millones al año en suscripciones mensuales y otros ingresos. Al respecto: DIBBEL, J.: «The life of the Chinese Gold Farmers», en *The New York Times Magazine,* 17 de junio de 2007. Disponible en: https://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html (visto 9-7-2019).

Ver Texto

(13) KNAUER, A.: ««Gold Farming» and the development of markets for virtual goods», en *Andeamus. University of California Honors Journal*, 2008, vol. 2, pág. 59.

Ver Texto

(14) DIBBEL, J.: «The life of the Chinese Gold Farmers», ob. cit.

Ver Texto

(15) KNAUER, A.: «Gold Farming» and the development…», ob. cit., pág. 59. El comercio paralelo de bienes virtuales procedentes de los juegos ha impulsado a sedes web como eBay o Yahoo Auctions, a crear la iniciativa VeRO Program (*Verified Rights Owner Program*), que pretende erradicar prácticas que violen los derechos de propiedad intelectual. Elabora una lista de los artículos virtuales que están protegidos legalmente y permite automáticamente que cualquiera de las empresas que dispongan de los derechos de propiedad intelectual y que participen en el programa puedan ordenar la retirada de los ítems de eBay cancelando las pujas que violan los derechos de autor. SUBIRANA, B. y CABAÑAS, M.: «Videojuegos MMORPG: los escenarios virtuales impactan con fuerza en el mundo real», en Cuadernos del EB Center, Barcelona, 2007, pág. 28.

Ver Texto

(16) DIBBEL, J.: «The life of the Chinese Gold Farmers», ob. cit.

Ver Texto

(17) CHECA GARCÍA, F.: «El uso de metaversos en el mundo educativo…», ob. cit., pág. 150.

Ver Texto

(18) AGUIRRE ROMERO, J. M.: «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI», en *Espéculo. Revista de estudios literarios*, 2004, disponible en http://www.ucm.es/info/especulo/numero27/cibercom.html (visto 1-7-2019).

Ver Texto

(19) AGUIRRE ROMERO, J. M.: «Ciberespacio y comunicación…», ob. cit.

Ver Texto

(20) CHECA GARCÍA, F.: «El uso de metaversos en el mundo educativo…», ob. cit., pág. 149.

Ver Texto

(21) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *Revista Electrónica de Ciencia Penal y Criminología*, 13-07 (2011), pág. 5.

Ver Texto

(22) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 8.

Ver Texto

(23) AGUIRRE ROMERO, J. M.: «Ciberespacio y comunicación…», ob. cit.

Ver Texto

(24) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 17.

Ver Texto

(25) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 8.

Ver Texto

(26) POSADA MAYA, R.: «El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual», en *Revista Nuevo Foro Penal,* vol. 13, nº. 88, enero-junio 2017, Medellín, pág. 80 y ss.

Ver Texto

(27) BRENNER, S.: «Is There Such a Thing as «Virtual Crime»?», en *California Law Review*, vol. 4 t. 1, 2001 , disponible en https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1077&context=bjcl (visto 2-7-2019).

Ver Texto

(28) Al respecto, Posada Maya califica esta forma de interpretar la naturaleza de los ciberdelitos como un «acto incomprensible de simplificación jurídica», que asimila equivocadamente estos delitos a aquellos en los que el autor utiliza de manera natural un instrumento físico ya que, en su opinión, el ciberespacio es mucho más que un medio o un instrumento, es una verdadera realidad simulada. POSADA MAYA, R.: «El cibercrimen y sus efectos…», ob. cit., pág. 90. En este sentido, no negamos el hecho de que estamos frente a un nuevo tipo de realidad, lo que no obsta a asumir que detrás de ella sigue habiendo un sujeto

que debe ser responsabilizado por sus actos.

Ver Texto

(29) POSADA MAYA, R.: «El cibercrimen y sus efectos…», ob. cit., pág. 88.

Ver Texto

(30) MIRÓ LLINARES, F.: *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid, 2012, pág. 39 y ss. Para analizar el cibercrimen el autor sugiere que se recurra a la teoría de las actividades cotidianas que prestan atención a la relación entre el cambio tecnológico y el cambio del crimen. En opinión de Miró Llinares, esta teoría resulta especialmente adecuada para analizar si las nuevas tecnologías conllevan la creación de un ámbito de oportunidad criminal nuevo y distinto.

Ver Texto

(31) BRENNER, S.: «Is There Such a Thing as «Virtual Crime»?», ob. cit.

Ver Texto

(32) Sobre las reformas incorporadas en 2015 sobre esta materia, ver: PIFARRÉ, M. J.: «Internet y redes sociales: un nuevo contexto para el delito» en *Revista de los Estudios de Derecho y Ciencia Política. Número Monográfico «Internet y redes sociales: un nuevo contexto para el delito»*, número 15 (noviembre de 2012), pág. 42. Contra esta opción se pronuncia Posada Maya alegando que esto delitos no se pueden reducir a un simple medio de ejecución de los verbos típicos en los delitos comunes. POSADA MAYA, R.: «El cibercrimen y sus efectos…», ob. cit., pág. 80.

Ver Texto

(33) No obstante, no existe acuerdo sobre la necesidad de que se verifique un contacto físico entre el autor y la víctima. Al respecto: CARUSO FONTÁN, M. V.: *Nuevas Perspectivas Contra la libertad sexual*, Valencia, 2006, pág. 201 y ss.

Ver Texto

(34) En opinión de García Álvarez, el «presenciar» debe interpretarse como exigencia de que la contemplación de los actos de naturaleza sexual por parte del menor sea directa. En opinión de esta autora, de no darse esta característica deberá recurrirse al delito del artículo 186 CP. GARCÍA ÁLVAREZ, P.: «La reforma de los capítulos II bis, IV y V del Título VIII del Código Penal en el Proyecto de Ley Orgánica de 20 de septiembre de 2013», en Muñoz Conde, F. (dir.): *Análisis de las reformas penales. Presente y futuro*, Valencia, 2015, pág. 159. Al respecto, Muñoz Conde considera que, si los hechos tuvieran lugar «online», seguirá aplicándose el artículo 183 bis mientras el menor visualice al autor en directo. MUÑOZ CONDE, F.: *Derecho Penal. Parte Especial*, Valencia , 2017, pág. 214. Si bien en este caso no se trata de la visualización directa de la imagen del autor, tampoco se puede considerar que el visionado corresponda a imágenes ajenas, puesto que el ingreso a un mundo virtual y la adopción de un avatar implica la asunción de una representación visual propia en el metaverso.

Ver Texto

(35) PASCUAL, J. A.: «¿Deben los hackers de videojuegos ir a la cárcel?», en *Computer Hoy*, 16 de junio de 2018, disponible en https://computerhoy.com/noticias/gaming/deben-hackers-videojuegos-ir-carcel-268969 (visto 10-7-2019).

Ver Texto

(36) CASAS HERRER, E.: *La red Oscura…,* ob. cit., pág. 208.

Ver Texto

(37) En 2007 la cadena BBC ha informado que la policía alemana se encontraba investigando acusaciones de que *Second Life* estaba siendo utilizada para comerciar con imágenes de abuso infantil. Al respecto: http://news.bbc.co.uk/2/hi/technology/6638331.stm. PARIS, N: «Virtual world 'child abuse' claim», en *The Telegraph*, 9 de mayo de 2007, disponible en https://www.telegraph.co.uk/news/worldnews/1551071/Virtual-world-child-abuse-claim.html (visto 10-7-2019).

Ver Texto

(38) Al respecto: LUNA, J. A.: «Rape Day», el videojuego en el que violar y matar a mujeres era «parte de la diversión» , en *El Diario.es*, 6 de marzo de 2019, disponible en https://www.eldiario.es/cultura/videojuegos/polemica-Rape-videojuego-mete-violador_0_874913436.html (visto 9-7-2019).

Ver Texto

(39) MARTÍNEZ, M. and MANOLOVITZ, T.: «Incest, Sexual Violence, and Rape in Video Games», 2009, disponible en http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.729.976, (visto 3-7-2019). Los autores explican que, a pesar de que los videojuegos pueden ser clasificados como «sólo para adultos», los productores de los mismos intentan evitar que el juego sea clasificado de esta manera, ya que ello reduce drásticamente las posibilidades de su distribución y, en consecuencia, de su venta.

Ver Texto

(40) Sobre este particular, ver: DILL, K. E.: «Violent Video Games, Rape Myth Acceptance, and Negative Attitudes toward Women», en *Violence Against Women in Families and Relationships: Volume 4, The Media and Cultural Attitudes*, 2009, disponible en https://www.researchgate.net/publication/258698138_Violent_Video_Games_Rape_Myth_Acceptance_and_Negative_Attitudes_toward_Women (visto 3-7-2019), págs. 125 y ss. La autora plantea que quienes juegan videojuegos violentos tienen más propensión a expresar actitudes negativas hacia las mujeres, siendo más probable que crean en el mito de la violación, es decir, que las mujeres tienen la fantasía de ser violadas.

Ver Texto

(41) Esta aseveración también ha sido utilizada para desviar la atención de otros problemas. Así, los medios periodísticos han resaltado el hecho de que el presidente norteamericano Donald Trump ha intentado desviar la atención sobre el problema del uso de armas de fuego en Estados Unidos, intentando culpar a los videojuegos de una matanza en Florida. OLLERO, D. J.: «La ciencia ha hablado: los videojuegos violentos no causan las matanzas escolares», en *El Mundo*, 22 de marzo de 2018, disponible en https://www.elmundo.es/papel/historias/2018/03/22/5ab273c2468aeb35128b465e.html (visto 11-7-2019).

Ver Texto

(42) CASAS HERRER, E.: *La red Oscura…,* ob. cit., pág. 207.

Ver Texto

(43) Al respect: KNAUER, A.: «Gold Farming» and the development…», ob. cit., pág. 61.

Ver Texto

(44) BIURRUM ABAD, F. J.: «Pokémon Go y su impacto en la 'legalidad aumentada», en *Actualidad Jurídica Aranzadi*, núm. 922/2016, Pamplona.

Ver Texto

(45) IZAGUIRRE OLMEDO, J.: «Análisis de los Ciberataques Realizados en América Latina», en *Research Journal* 2018, vol. 3, No. 9, pág. 185.

Ver Texto

(46) Una de las características propias de estos videojuegos es que su mundo es persistente, el decir, el juego prosigue su devenir y evoluciona, cambia y se transforma pese a que el jugador no esté conectado. Esta persistencia puede implicar una cierta obligación de jugar. Además, se trata se juegos que están disponibles y accesibles las 24 horas del día, los 7 días de la semana. Estas circunstancias favorecen el desarrollo de una conducta adictiva. De hecho, el DSM5 contempla en la Sección III la adicción a los videojuegos y no otras posibles adicciones tecnológicas. Según esta clasificación se trata de una «adicción conductual». En el DSMIV y en el DSM-IV-TR se incluía el juego patológico en el apartado de «Trastornos del control de impulsos no clasificados en otros apartados». Esta tendencia ha cambiado y en el DSM5 se incluye en el apartado de «*Substanced related and addictive disorders*» con el argumento de que las

conductas de juego activan sistemas de recompensa similares a los que activan la drogas y producen síntomas conductuales comparables a los producidos por sustancias. CARBONELL, X.: «La adicción a los videojuegos en el DSM-5», en *Adicciones*, vol. 26, nº 2, 2014, pág. 91.

Ver Texto

(47) BRENNER, S.: «Is There Such a Thing as «Virtual Crime»?», ob. cit.

Ver Texto

(48) CASAS HERRER, E.: *La red Oscura…,* ob. cit., pág. 206.

Ver Texto

(49) Pueden verse en youtube videos caseros con títulos como «Chinese Gold Farmers must die» https://www.youtube.com/watch?v=Tt08MtzRhrg (visto 9-7-2019).

Ver Texto

(50) DIBBEL, J.: «The life of the Chinese Gold Farmers», ob. cit.

Ver Texto

(51) GARCÍA SAN NARCISO, M.: «Acoso a las «gamers»», en *El Periódico*, 23 de julio de 2017, disponible en https://www.elperiodico.com/es/sociedad/20170723/usuarias-de-los-videojuegos-denuncian-el-acoso-que-sufren-6185779, (visto 18-7-2019).

Ver Texto

(52) OTTO, C.: «Acoso, boicot y ninguneo: el videojuego español tiene un problema de machismo», en *El Confidencial*, 25 de julio de 2017, disponible en https://www.elconfidencial.com/tecnologia/2017-07-09/machismo-gaming-blissy-gaming-ladies -todas-gamers-flipin_1409643/ (visto 18-7-20199).

Ver Texto

(53) GARCÍA, F.: «El acoso en los videojuegos online» en *As*, 4 de julio de 2017, disponible en https://as.com/meristation/2017/03/24/noticias/1490310840_163921.html (visto 18-7-2019).

Ver Texto

(54) GARCÍA, F.: «El acoso en los videojuegos online», ob. cit.

Ver Texto

(55) «Corea del Sur sanciona el "boosting" en los videojuegos», disponible en https://www.economiadigital.es/tecnologia-y-tendencias/corea-del-sur-sanciona-el-boosting-en-los-videojuegos_594287_102.html (visto 12-7-2019).

Ver Texto

(56) Este artículo se encuentra en consonancia con el Convenio del Consejo de Europa sobre Manipulación de Competiciones Deportivas, que en su artículo 15 establece que «*Cada Parte se cerciorará de que su legislación nacional permite imponer sanciones penales a la manipulación de competiciones deportivas cuando lleve consigo prácticas coercitivas, corruptas o fraudulentas, según las definan las leyes nacionales*». Sobre esta normativa, ampliamente: PÉREZ GONZÁLEZ, C.: «A propósito de la acción del Consejo de Europa en el ámbito del deporte: análisis del convenio europeo sobre la manipulación de competiciones deportivas», en *Eunomía. Revista en Cultura de la Legalidad*, nº 8, marzo-agosto 2015, págs. 71-92.

Ver Texto

(57) MARTÍN, R. P.: «Así es la Liga de Videojuegos Profesional en España» en *El Diario.es*, 24 de julio de 2017, disponible en https://www.eldiario.es/ping/Liga-Videojuegos-Profesional-Espana_6_636646346.html

(visto 25-7-2019).

Ver Texto

(58) KINDHÄUSER, U.: «Presupuestos de la corrupción punible en el Estado, la economía y la sociedad. Los delitos de corrupción en el Código Penal alemán», en *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, núm. 3, Chile, 2007, pág . 15.

Ver Texto

(59) Parece manifestarse en contra de esta opinión Malam Seña, quien resalta el papel que desempeña el deporte en nuestras sociedades y los intereses involucrados: MALAM SEÑA, J. F.: «La corrupción en el deporte», en *Fair Play. Revista de Filosofía, Ética y Derecho del deporte*, vol. 2, nº 2, 2014, pág. 120. También en este sentido: DÍEZ GARCÍA, J.: «La importancia de la transparencia y la protección del deporte por parte de los poderes públicos», en *Revista Internacional. Transparencia y Seguridad*, nº 5 septiembre-diciembre 2017, págs. 1-10.

Ver Texto

(60) Las 40 Recomendaciones del GAFI (Grupo de Acción Financiera Internacional) alertan y previenen de estos peligros (ver Recomendación 15). FATF (2012-2019), «International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation», FATF, Paris, France, disponible en http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (visto 17-7-2019). Al respecto: ABEL SOUTO, M.: «Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y reforma penal», en *Revista Electrónica de Ciencia Penal y Criminología*, 14-14 (2012), págs. 1-45.

Ver Texto

(61) En su propia página web *Entropia Universe* se define como un entorno virtual avanzado en línea 3D con un sistema planetario desarrollado y un sistema económico de dinero real en efectivo de carácter universal, donde cada planeta ofrece una amplia variedad de entretenimiento emocionante de forma que se puede viajar entre los planetas a través del espacio y socializar con personas de todo el mundo. Disponible en https://www.entropiauniverse.com/entropia-universe/. Visto 9-7-2019.

Ver Texto

(62) IRWIN, A. S. M. y SLAY, J.: «Detecting Money Laundering and Terrorism Financing…», ob. cit., pág. 43.

Ver Texto

(63) SULLIVAN, K.: «Virtual Money Laundering and Fraud Second Life and Other Online Sites Targeted by Criminals», disponible en https://www.bankinfosecurity.com/virtual-money-laundering-fraud-a-809 (visto 9-7-2019).

Ver Texto

(64) LEAPMAN, B.: «Second Life world may be heaven for terrorists», en *The Telegraph*, 13 de mayo de 2007. Disponible en https://www.telegraph.co.uk/news/uknews/1551423/Second-Life-world-may-be-haven-for-terrorists.html (visto 9-7-2019).

Ver Texto

(65) SANDERS, M.: «Money laundering through gold farming and virtual goods», 3 June 2009, citado por IRWIN, A. S. M. y SLAY, J.: «Detecting Money Laundering and Terrorism Financing…», ob. cit., pág. 43.

Ver Texto

(66) OTERO, C.: «Así usan el videojuego Fortnite para blanquear dinero los cibercriminales», en *As*, 21 de enero de 2019, disponible en ttps:/ /as.com/meristation/2019/01/21/betech/1548092120_623300.html (visto 17-7.2019). Fornite no es el único juego en el que se utilizan estos métodos. La empresa de Seguridad *Kromtech* ha localizado y puesto de manifiesto una serie de blanqueos que se producen utilizando los juegos *Clash of Clans, Clash Royale* y *Marvel Contest of Champions.* En junio de 2018, la empresa descubrió una extraña base de datos expuesta públicamente en Internet sin necesidad de contraseña junto con una gran cantidad de números de tarjetas de crédito e información personal en el interior. Cuando la examinaron notaron que esta base de datos parecía pertenecer a ladrones de tarjetas de crédito y que era relativamente nueva, solo tenía unos pocos meses. En una de las tablas encontraros enlaces a cuentas de Facebook. De esas cuentas, se localizaron enlaces a una página de Facebook en

publicidad vietnamita, se trata de una «herramienta» especial, que también tenía unos pocos meses. Según sus estimaciones, el sistema procesó aproximadamente 20,000 tarjetas de crédito robadas en solo un mes y medio (desde finales de abril de 2018 hasta mediados de junio de 2018). Estos ladrones de tarjetas de crédito sólo estaban apuntados a los tres juegos mencionados. DIACHENKO, B.: «Digital Laundry: how credit card thieves use free-to-play apps to launder their ill-gotten gains», 16 de Julio de 2018, disponible en https://kromtech.com/blog/security-center/digital-laundry (visto 17-7-2019). Kromtech es una compañía de software establecida en 2007, que produce e integra software de tecnología avanzada en los campos de Sistemas de control de acceso y Auditoría y seguridad de próxima generación, entre otros. (https://krontech.com/about-us/, visto 17-7-2019). El periódico «El Mundo» también ha informado sobre una operación de características similares en los juegos *FIFA* y *Mass Effect*: *El Mundo*, 16 de noviembre de 2016, disponible en https://www.elmundo.es/tecnologia/2016/11/16/582c289046163f820d8b460b.html (visto 17-7-2019).

Ver Texto

(67) «Así se blanquea dinero con Fortnite», en *El Mundo*, 15 de enero de 2019, disponible en https://www.elmundo.es/tecnologia/2019/01/15/5c3cae12fc6c83b8078b45d2.html (visto 17-7-2019). El periódico informa que según la firma de seguridad Sixgill, eBay ha procesado ventas por el valor de 220.000 euros en 60 días. Del mismo modo, la aparición del juego en compras producidas en la «*dark web*» también ha aumentado exponencialmente a medida que *Fortnite* se ha vuelto más popular.

Ver Texto

(68) LÓPEZ JIMÉNEZ, J. M.: «Monedas virtuales y prevención del blanqueo de capitales», en *Málaga y Cervantes: La espada y la Pluma. X Jornadas de Seguridad, Defensa y Cooperación. El Fenómeno terrorista y su incidencia en el Mediterráneo (Similitudes entre dos épocas históricas)*, Málaga, 2017, pág. 69. En similar sentido: ZUÑIGA, A.: «Bitcoin: mucho más que una moneda», en *Escritura Pública*, nº 92, 2015, pág. 57.

Ver Texto

(69) CASAS HERRER, E.: *La red Oscura…,* ob. cit., pág. 25.

Ver Texto

(70) CASAS HERRER, E.: *La red Oscura…*, ob. cit., pág. 37.

Ver Texto

(71) «Evaluación de la Amenaza de la Delincuencia Organizada en Internet» (IOCTA), disponible en https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (visto 17-7-2019).

Ver Texto

(72) POSADA MAYA, R.: «El cibercrimen y sus efectos…», ob. cit., pág. 90.

Ver Texto

(73) RAYÓN BALLESTEROS, M. C. y GÓMEZ HERNÁNDEZ, J. A.: «Cibercrimen: particularidades en su investigación y enjuiciamiento», en Anuario Jurídico y Económico Escurialense, XLVII (2014), pág. 218.

Ver Texto

(74) Disponible en http://www.europarl.europa.eu/doceo/document/A-8-2016-0168_ES.html#title1 (visto 18-7-2019).

Ver Texto

(75) CASAS HERRER, E.: *La red Oscura…*, ob. cit., pág. 212 y ss. Sobre los riesgos que enfrenta *Bitcoin* también ver: DOMINGUEZ JURADO, J. M. y GARCÍA RUIZ, R.: «Blockchain y las criptomonedas: el caso bitcoin», en Revista de los Estudios de Economía y Empresa. Oikonomics, nº 10, noviembre de 2018, pág. 69.

Ver Texto

(76) Evaluación de la Amenaza de la Delincuencia Organizada en Internet (IOCTA), disponible en https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment (visto 17-7-2019).

Ver Texto

(77) Para una completa explicación del funcionamiento del sistema de cadena de bloques que da lugar al valor de esta criptomoneda, ver: CASAS HERRER, E.: *La red Oscura…*, ob. cit., pág. 212. FERNÁNDEZ, A. y ALONSO, A.: «La extraña historia del bitcoin» en *Tiempo*, nº 1632, 8 de enero de 21014, págs. 42-43. RODRÍGUEZ HERRERA, D.: «¿Qué es Bitcoin?» en *La Ilustración liberal. Revista española y americana*, nº 59, 2014. MONCADA, I.: «Bitcoin, ¿el dinero del futuro?» en *Anales de Mecánica y Electricidad*, marzo-abril 2013, págs. 24-30. Sobre otros posibles usos del *Blockhaim*: HAERINGER , G. y HALABURDA, H: «Bitcóin: ¿una revolución?», en *Papeles de Economía Española*, nº 157, 2018, pág. 248.

Ver Texto

(78) ARMAS VEGA, E. A. y otros: «Alternativas a Bitcoin y su Uso en el Cibercrimen» en *Actas de las Cuartas Jornadas Nacionales de Investigación en Ciberseguridad*, Donostia-San Sebastián, Guipúzcoa, 13-15 de Junio, 2018, págs. 107 y 108. Incluso Facebook ha anunciado recientemente que contará con su propia moneda que se llamará Libra. Se tratará de una criptomoneda de baja volatilidad basada en un *blochaim* descentralizado y tendrá como objetivo principal llegar a las personas que no tienen una cuenta bancaria, para que puedan ahorrar pagar o enviar transferencias a un coste bajo. Libra estará apoyada por una reserva real y podrá cambiarse por otras monedas reales en base a una tasa estable de cambio. PÉREZ COLOMÉ, J.: «Facebook lanza libra, su propia moneda para «reinventar el dinero» en *El País*, 19 de junio de 2019, disponible en https://elpais.com/tecnologia/2019/06/18/actualidad/1560851467_183722.html (visto 17-7-2019).

Ver Texto

(79) NIETO GIMÉNEZ-MONTESINOS, M. A. y HERNÁEZ MOLERA, J.: «Monedas virtuales y locales: las paramonedas, ¿nuevas formas de dinero?», en *Banco de España, Revista de Estabilidad Financiera*, núm. 35, 2018, pág. 120. Sobre la polémica de una posible regulación de las monedas virtuales , ampliamente: NAVAS NAVARRO, S.: «Un mercado financiero floreciente: el del dinero virtual no regulado (Especial atención a los BITCOINS)» en *Revista CESCO de Derecho de Consumo*, Nº 13/2015, págs. 79-115.

Ver Texto

(80) Por otro lado, también se ha puesto de manifiesto que el desarrollo de *Bitcoin* genera efectos físicos a gran escala, especialmente en términos de consumo energético y huella de carbono. BARAONA POHL, E. y REYES NAJERA, C.: «El peso de Bitcoin», en *ARQ 98*, Santiago de Chile, 2018, págs. 32-43.

Ver Texto

(81) Disponible en https://www.boe.es/doue/2018/156/L00043-00074.pdf (visto 18-7-2019).

Ver Texto

(82) El 8 de febrero de 2018 la CNMV y del Banco de España emitieron un comunicado conjunto sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs). En este comunicado advierten que, hasta la fecha, ninguna emisión de «criptomoneda» ni ninguna ICO ha sido registrada, autorizada o verificada por ningún organismo supervisor en España. Esto implica que no existen «criptomonedas» ni «tokens» emitidos en ICOs cuya adquisición o tenencia en España pueda beneficiarse de ninguna de las garantías o protecciones previstas en la normativa relativa a productos bancarios o de inversión. . Disponible en file:///D:/Usuarios/vcaruso/Dropbox/Word%20of%20Warcrarft/Bibliografia/lavado%202/nuevo/bitcoin/banco%20de%20espa%C3%B1a%20presbe2018_07.pdf (visto 17-7-2019).

Ver Texto

(83) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 25.

Ver Texto

(84) RAYÓN BALLESTEROS, M. C. y GÓMEZ HERNÁNDEZ, J. A.: «Cibercrimen: particularidades en su investigación y enjuiciamiento», ob. cit., pág. 233.

Ver Texto

(85) DE LUCA, S. y DEL CARRIL, E.: «Cooperación internacional en materia penal en el Mercosur: el cibercrimen», en *Revista de la Secretaría del Tribunal Permanente de Revisión*, año 5, nº 10, Octubre 2017, pág. 23.

Ver Texto

(86) Al respecto: LEZERTÚA, M.: «El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa - proteger el ejercicio de derechos fundamentales en las redes informáticas», en *Cuadernos Europeos de Deusto*, núm. 25/2001, Bilbao, pág. 93.

Ver Texto

(87) Al respecto: AGUILAR CÁRCELES, M. M.: «Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido», en *Revista Criminalidad*, 57 (1), pág. 127. PONS GAMÓN, V.: «Internet , la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad», en *URVIO. Revista Latinoamericana de Estudios de Seguridad*, nº. 20, Quito, junio 2017, pág. 90.

Ver Texto

(88) CASAS HERRER, E.: La red Oscura…, ob. cit., pág. 174 y ss.

Ver Texto

(89) CASAS HERRER, E.: La red Oscura…, ob. cit., pág. 174 y ss.

Ver Texto

(90) MIRÓ LLINARES, F.: *El Cibercrimen. Fenomenología y criminología*…, ob. cit. 243.

Ver Texto

(91) Al respecto: POSADA MAYA, R.: «El cibercrimen y sus efectos…», ob. cit., pág. 103.

Ver Texto

(92) RAYÓN BALLESTEROS, M. C. y GÓMEZ HERNÁNDEZ, J. A.: «Cibercrimen: particularidades en su investigación y enjuiciamiento», ob. cit., pág. 230.

Ver Texto

(93) LEZERTÚA, M.: «El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa…», ob. cit., pág. 87.

Ver Texto

(94) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 38.

Ver Texto

(95) RAYÓN BALLESTEROS, M. C. y GÓMEZ HERNÁNDEZ, J. A.: «Cibercrimen: particularidades en su investigación y enjuiciamiento», ob. cit., pág. 230.

Ver Texto

(96) MIRÓ LLINARES, F.: «La oportunidad criminal en el ciberespacio…», ob. cit., pág. 40.

Ver Texto