ADI 43 (2023): 109-131

EL *CYBERSQUATTING* DEL SIGLO XXI: NUEVOS DESAFIOS PARA EL DERECHO DE MARCAS

CYBERSQUATTING OF THE 21ST CENTURY: NEW CHALLENGES FOR TRADEMARK LAW

Mónica Lastiri Santiago*

RESUMEN

Desde que la Organización Mundial de la Propiedad Intelectual (OMPI) comenzó a mediar en los conflictos de los nombres de dominio en Internet en el año 1999, esta práctica maliciosa de apropiación ha llegado a cifras históricas en el último año 2022. Con ello, han nacido nuevas tácticas de ciberocupación que dejan cuestiones jurídicas por resolver.

Palabras clave: *cybersquatting*, nombres de dominio y marcas.

ABSTRACT

Since the World Intellectual Property Organization (WIPO) began mediating Internet domain name disputes in 1999, this malicious practice of domain name grabbing has reached record in the past year, 2022, and thus, new cybersquatting practices have been born that leave legal issues to be resolved.

Keywords: cybersquatting, domain names and trademarks.

* Profesora Dra. Visitante de Derecho Mercantil de la Universidad Carlos III de Madrid (*mlastiri@der-pr.uc3m.es*). Código Orcid 0000-0001-6815.5728. Este artículo se ha realizado bajo el «Proyecto PID2020-114549RB-100, Empresa y Mercados: (R)evolución digital, integridad y sostenibilidad, y su asimilación por el Derecho Privado, Regulatorio y de la Competencia».

Fecha de recepción: 19 de abril de 2023 // Fecha de aceptación: 19 de abril de 2023.

I. EL ORIGEN DEL *CYBERSQUATTING* DE NOMBRES DE DOMINIO Y SU REPERCUSIÓN EN EL DERECHO DE MARCAS

El *cybersquatting* o ciberocupación constituye el primer desafío al que se tuvo que enfrentarse el Derecho con la llegada de Internet. En la actualidad es fundamental la presencia digital de las empresas en la Red. Tener un sitio web es tan importante como tener la sede física del negocio. Por tanto, el nombre de dominio se convierte es una pieza esencial.

El *cybersquatting* comenzó con el registro de infinidad de marcas conocidas como nombres de dominio. Consiste en el registro, la venta y el uso de un nombre de dominio con la intención de enriquecerse a costa del prestigio de marcas registradas. En este siglo XXI consiste en registrar un nombre de dominio que sea muy similar a uno ya existente, especialmente los que incorporan marcas conocidas por el público consumidor. Lo anterior, con fin de aprovechar el renombre de estas para fines ilícitos.

Para poder profundizar en este fenómeno, resulta fundamental referirnos al término *cybersquatter,* pues en su significado se basa la totalidad de la regulación que atañe al nombre de dominio.

Cybersquatter[1] deriva del término anglosajón *squatter,* que significa «usurpador», y hace referencia a una persona que se establece sin tener derecho a ello en un terreno público o en una propiedad que no se utiliza[2].

En el ámbito de los nombres de dominio, el término *cybersquatter* fue utilizado por primera vez para hacer referencia a aquellos solicitantes de registros de dominios que habían sido «dados de baja» por negarse a pagar las tasas de registro o de renovación[3]. Más adelante se utilizó para denominar a aquellas personas que registran de forma abusiva, deliberada e indiscriminadamente nombres de dominio sin tener interés legítimo y que además son coincidentes con marcas

---

[1] Los *cybersquatters* reciben también la calificación de cuatreros de Internet, ciberusurpadores, okupas del ciberespacio o piratas de nombres de dominio. *Vid.* RAMOS HERRANZ (2004), pág. 209.

[2] «Squatters are people who live in an unused building without having a legal right to do so», *BBC English Dictionary,* HarperCollins Publishers, Londres, 2009, p. 1094. Igualmente, *vid.* el significado del término «*squatter*» en *http://dictionary.reference.com/browse/squatter,* y en Property Law ChadBoard, «What is a squatter? What rights does a squatter have?», *http://counsel.net/chatboards/property/topic39/5.20.08.11.28.50.html* (visita: 10 de abril de 2023).

[3] NELMARK (2004-2005), pág. 10.

registradas por terceras personas. Ello con el fin de solicitar cantidades elevadas de dinero a su legítimo titular por la transmisión de los mismos[4]. Otro calificativo para nombrar a este tipo de usuario es el de *domain names dealers*[5], aunque el que ha prevalecido ha sido el de *cybersquatters.*

En 1996, el Tribunal del Distrito Norte de Illinois conoció el caso *Intermatic Inc. vs. Toeppen*[6], donde por primera vez se hacía referencia al término *cybersquatter* en el sentido que lo conocemos ahora. Hasta el momento del juicio, Dennis Toeppen, el demandado, había registrado más de 240 nombres de dominio, la mayoría de los cuales coincidían con nombres de conocidas empresas[7]. En este asunto, el juez calificó al demandado como *cybersquatter,* definiendo el término como aquel individuo que intenta beneficiarse de Internet registrando y luego revendiendo o licenciando nombres de dominio a las empresas, que invierten millones de dólares para adquirir la notoriedad y buena fama de sus marcas[8].

En este asunto, Toeppen fue considerado un *squatter* en el entendido de que nunca tuvo los derechos de la marca «Intermatic», siguiéndose con la idea de que un titular de marca posee todos los derechos sobre la misma.

Posteriormente y, como era de esperarse, Dennis Toeppen fue protagonista de muchas de las primeras demandas sobre ciberocupación. Una de ellas fue la interpuesta por la empresa norteamericana Panavision International por el registro del nombre de dominio *panavision.com*. Dicha empresa era titular de la marca «Panavision», y al verse imposibilitada de disponer de un nombre de dominio igual por haberlo registrado previamente Toeppen, le instó a que se lo cediera, en virtud de que tenía derechos anteriores sobre la marca. Toeppen respondió que el registro de dominio no constituía uso de marca y ofreció la cesión del nombre de dominio a cambio de 13.000 dólares. Panavision rechazó la oferta y emprendió acciones judiciales para recuperar el nombre de dominio.

Este caso lo conoció el Tribunal de Distrito de California y terminó en el Tribunal de Apelaciones del Noveno Circuito, que estableció que las acciones de Toeppen violaban la Federal Trademark Dilution Act de 1995 y el Anti-dilution Statute, California Business.

II. LA IMPORTANCIA DEL TÉRMINO *CYBERSQUATTER* EN MATERIA DE NOMBRES DOMINIO

La ciberocupación se desarrolla de forma similar al entorno en que se desenvuelve. Esta práctica predatoria y parasitaria evolucionó a una velocidad pasmo-

---

[4] Gilwit (2003), pág. 267.

[5] Carbajo Cascón (2002), pág. 114.

[6] Intermatic Incorporated vs. Dennis Toeppen 1996 U.S. Dist. Lexis 14878 (D.III. 1996), *https://casetext.com/case/intermatic-inc-v-toeppen* (visita: 10 de abril de 2023).

[7] En esos registros figuran *deltaairlines.com, eddiebauer.com, neimanmarcus.com*. *Vid.* Committee On The Judiciary United States Senate. Cybersquatting and Consumer Protection: Ensuring Domain Name Integrity: Hearing on S. 1255 Before the Senate Comm. On the Judiciary, 106th Cong. 1 (1999), pág. 10. Disponible en *http://www.gpo.gov/fdsys/pkg/CHRG-106shrg67164/pdf/CHRG-106shrg67164.pdf* (visita: 10 de abril de 2023), pág. 7.

[8] «*An individual who attempt [s] to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark*». *Vid. Intermatic Incorporated vs. Dennis Toeppen*.

sa, sorprendiendo a más de una gran empresa que ignoraba el enorme potencial del ámbito digital.

Pero el asombro se convirtió rápidamente en preocupación cuando esas grandes compañías se dieron cuenta de la formidable oportunidad comercial que nacía con Internet, pero el nombre de sus empresas, junto con sus marcas más valoradas, estaban ya registradas como nombres de dominio. Esto impedía o dificultaba su entrada a Internet y, por consiguientes, sus oportunidades comerciales en este ámbito desmaterializado.

El crecimiento de la ciberocupación fue inmediato; tanto que los ordenamientos jurídicos fueron incapaces de reaccionar a tiempo para evitar su progresión. Por ello, las empresas buscaron alternativas que pudiesen permitirles la entrada a la Red de forma rápida, sin desperdiciar tiempo valioso para poder ejercer el comercio electrónico.

Entre las soluciones urgentes surgieron los acuerdos económicos privados con los *cybersquatters,* por medio de los cuales estos les cedían el nombre o los nombres de dominio de forma expedita a cambio de una cantidad importante de dinero. Estos acuerdos se evidenciaron como necesarios, además, por el hecho de que pese a que los legítimos titulares de marcas, en virtud de la legislación protectora de signos distintivos, podían entablar acciones judiciales contra los *cybersquatters,* los costes de los litigios contra un número infinito de acusados constituían un desincentivo importante. A menudo, el gran número de casos obligaba a los titulares de marcas a presentar demandas múltiples en uno o más órganos jurisdiccionales, por lo que, en muchos casos, los titulares de marcas optaban por la vía rápida de negociar con el *cybersquatter*.

La premura en la obtención del nombre de dominio por parte de los titulares de marcas se debía a las pérdidas económicas que podía implicar el adoptar los remedios legales tradicionales, que traían aparejados incertidumbre, gastos e inseguridad jurídica, ya que al no contemplarse en la legislación situaciones similares, corrían el riesgo de emprender una lucha que les llevaría tiempo y que, en consecuencia, impedía el ingreso inmediato en Internet. Debido a su falta de adaptación a un medio tan innovador, en muchos casos los remedios jurídicos tradicionales se mostraron como mecanismos demasiado lentos o formalistas para poder tratar adecuadamente el fenómeno de la ciberocupación[9].

Este problema se produjo por la falta de conexión entre los fines para los que se diseñó el sistema de nombres de dominio y aquellos para los que existe la propiedad industrial. Este alejamiento dio origen a numerosas controversias, en ocasiones motivadas por la pura y simple piratería, a coincidencias ocasionales o a ciertas colisiones con derechos correctamente constituidos, las cuales no podían ni pueden ser resueltas exclusivamente por la legislación de marcas, que no contemplaba, como es normal, el fenómeno de los nombres de dominio.

A pesar de la ausencia de alternativas jurídicas, hubo empresas que, partiendo de la absoluta certeza de que estaban siendo víctimas de una flagrante violación de sus derechos de propiedad industrial, se negaron a ceder ante los atropellos de los *cybersquatters* y emprendieron su lucha utilizando el esquema

[9] Agustinoy Guilayn (2002), pág. 69.

jurídico tradicional de marcas que, como poco, ofrecía una protección jurídica a sus signos distintivos.

Por ello, desde un primer momento, el tratamiento legal del *cybersquatting* fue enfocado como una invasión del derecho de marca, aplicándose instituciones y legislación propias de este ámbito para la resolución de las controversias [10].

Debido a que los nombres de dominio son un fenómeno que nació en Estados Unidos, fue este país el pionero en la aplicación de la legislación de marcas para remediar los conflictos surgidos entre los titulares de marcas y los *cybersquatters* [11]. No obstante, la aplicación del derecho de marcas fue poco exitosa debido a la naturaleza digital del nombre de dominio.

III. EL *CYBERSQUATTING* DEL SIGLO XXI

El eje sobre el que gira la ciberocupación son los nombres de dominio y como hemos podido constatar, la problemática jurídica de este fenómeno se ha centrado en su conflicto con las marcas. Ese registro abusivo de marcas como nombres de dominio ha sido la razón por la cual se ha creado una serie de instrumentos jurídicos y políticas con el fin de salvaguardar el derecho de los titulares de marcas en el ámbito digital.

El examen de los problemas suscitados entre las figuras mencionadas ha sido tratado con solvencia en la literatura jurídica nacional y extranjera, por lo que contamos con valiosas aportaciones por parte de la doctrina [12]. Sin embargo, el *cibersquatting* además de estar yendo en aumento, ha ido adquiriendo matices distintos que los distancian de la práctica habitual del sólo el registro, venta con el fin de aprovecharse del prestigio de las marcas.

La evolución histórica de los nombres de dominio está unida al desarrollo tecnológico, a su importancia como activo empresarial y a la relevancia económica que ha adquirido como llave de entrada a Internet y al comercio establecido en ella. Por lo anterior, en la actualidad el *cybersquatting* es la acción y efecto de registrar un nombre de dominio sabiendo que otro ostenta un mejor derecho. Dicho registro se hace con el propósito de extorsionar a aquel que tiene el derecho o bien simplemente se registra con el fin de desviar el tráfico web hacia un sitio web no deseado por el usuario y por ello el que lo registra obtiene beneficios económicos de forma ilícita.

IV. LAS NUEVAS MANIFESTACIONES DEL *CYBERSQUATTING*

El cambio al teletrabajo y la transición a los eventos sociales virtuales, intensificados por la restricción del movimiento físico y los espacios públicos durante la pandemia contribuyeron al aceleramiento de la dependencia de las

---

[10] *Ibid.,* pág. 79.

[11] Para mayor información acerca del derecho de marcas estadounidense, *vid.* Callmann (1981); McCarthy (1997); Gilson, J. y Samuels (2003); Flinn (2000); Gilson y y Gilson (2005).

[12] De Miguel Asensio (2002); Sanz de Acedo Hecquet (2001); Sammarco (2002); Massaguer Fuentes (1997), entra muchas otras obras. Información sobre más literatura sobre el tema, *vid.* Lastiri Santiago (2014), pág. 57.

personas en las experiencias digitales. Por ello, se intensificó el *e-commerce* y la necesidad de tener presencia en ese escenario. Para lograr ese objetivo es absolutamente imprescindible registrar un nombre de dominio.

Recordemos que la importancia del nombre de dominio descansa sobre dos funciones fundamentales. La primera es la social, porque son el elemento esencial para el correcto funcionamiento y desarrollo de la sociedad de la información, ya que, por medio del mismo, se logra una perfecta identificación y localización de las personas a través de sus ordenadores. Y la segunda, es la económica, porque es el activo digital más valioso para las empresas. Esto se debe a que no existe negocio que no pretenda tener presencia en Internet y para ello es esencial el registro de un nombre de dominio. Lo anterior, convierte a esta figura en la llave de acceso a la red.

Estas dos importantes misiones son la razón por la cual los *cyberquatters* han creados nuevas vías para obtener el control del nombre de dominio y así obtener beneficios económicos de forma ilícita. Por ello, los titulares de marcas continúan haciendo frente a la amenaza permanente de los *cybersquatters* que se apropian indebidamente de sus marcas, registrándolas como nombres de dominio. Ello acudiendo a novedosas formas de ciberocupación. Entra las que podemos mencionar, está la distribución de programas de *malware*[13] o participar en campañas de *phishing* o fraude por Internet. Son varias las formas actuales de *cybersquatting*. Entre las que podemos mencionar:

1. El *phishing* de nombres de dominio

El *phishing* es una actividad delictiva que utiliza técnicas de ingeniería social. Los *phishers* intentan adquirir información confidencial de manera fraudulenta, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por una entidad confiable en una comunicación electrónica[14].

Concretamente, e*l phishing* de nombres de dominio es una práctica abusiva que puede causar enormes daños a los titulares de marcas y a los consumidores. Es un tipo de SCAM (estafa *online*) que consiste en enviar un *e-mail* de aviso de renovación del dominio al registrante. En el *e-mail* fraudulento se informa sobre la próxima renovación, y se proporciona un *link* para pagar dicha renovación. La finalidad del fraude es conseguir los datos de las tarjetas mientras todo el proceso simula la renovación del nombre de dominio (que nunca se lleva a cabo).

Normalmente este tipo de *e-mails* fraudulentos son enviados como asuntos llamativos, como, por ejemplo, «*Domain Name Renewal*»[15]. En numerosas ocasiones, los correos electrónicos de *phishing* dirigidos a los registrantes aparentan haber sido enviados por la *Internet Corporation for Assigned Names and Numbres* (ICANN), conteniendo el logotipo, imagen institucional y su nombre en la dirección electrónica del remitente pese a que ICANN nunca envía correos

---

[13] Un *software* que realiza funciones maliciosas o no deseadas una vez instalado.

[14] Mihai (2012), pág. 62.

[15] ANW, «Phising de dominios», en *https://www.anw.es/blog/phishing-de-dominios/* (visita: 10 de abril de 2023).

directamente a los registrantes en relación con sus nombres de dominio y tampoco solicita pagos o tarifas [16].

2. *Typosquatting*

El *typosquatting* es considerado como una forma de *cybersquatting*. Se define como la alteración de la literalidad de la denominación de la marca con la intención de generar confusión con el signo distintivo original [17].

Los *typosquatters* registran nombres de dominio que son premeditadas faltas de ortografía o errores en la denominación de la marca notoria o renombrada para obtener provecho de su reputación [18]. La intención es la obtención de beneficios económicos, ya sea mediante la venta del nombre de dominio al titular del derecho de marca o el cobro de un canon por redirigir a los visitantes hacia su página web [19], o bien comercializando bienes o servicios, mediante publicidad, a través del parking de dominios [20] o simplemente creando sus propias webs para generar tráfico en las mismas [21].

El *typosquatting* se concreta en la práctica de varias formas:

— Registrando un error universal de escritura o falta de ortografía en la denominación incorporada en el SLD [22], como *www.microsokt.com* en lugar de *www.microsoft.com,* o *www.berizon.com* en lugar de *www.verizon.com.*

— Prescindiendo de alguna letra de la marca famosa, como en *www.ingdirec.com,* en lugar de *www.ingdirect.es.*

— Generando distintas formas de la palabra, como *www.cnncom.org* o *www.wwwcnn.com* en lugar de *www.cnn.com* [23].

En definitiva, el *typosquatting* consiste en la transposición de alguna letra (o dígito) de la marca, la aparente transcripción errónea de la misma, la inversión de algunos de sus elementos, o bien la adición a la marca previa de algún elemento, ya sea una letra o una palabra [24].

---

[16] ICCAN, «PART. IV. Identifying phishing scams, DNSSEC-Signing and another tips to protect your domain name», 30 de abril de 2020, *https://www.icann.org/es/blogs/details/do-you-have-a-domain-name-heres-what-you-need-to-know-30-4-2020-es* (visita: 10 de abril de 2023).

[17] Soler Masota (2004), pág. 19. En el mismo sentido, *vid.* Slavin (2004).

[18] Un caso paradigmático de *typosquatting* fue el que enfrentó a *Shields vs. Zuccarini,* 254 F. 3d 476, 483 (3d. Cir. 2001), disponible en *http://scholar.google.com/scholar_case?case=3776366602637795017&q=Shields+v.+Zuccarini&hl=en&as_sdt=2002* (visita: 10 de abril de 2023). Para un análisis sobre este asunto, *vid.* Clark (2003), págs. 1491-1492; Gilwit (2003), págs. 287 y ss.

[19] Soler Masota (2004), pág. 20.

[20] Es un sistema de gestión de publicidad insertada en los nombres de dominio. Funciona de forma idéntica al ya mencionado negocio del *pay-per-click advertising*. *Vid.* Herrador Muñoz (2014). Permite redirigir un nombre de dominio que no tiene un sitio web en marcha a una página web que contiene únicamente publicidad relacionada con el significado del SLD, de modo que cuando un usuario localiza el dominio «aparcado» puede generarle ingresos económicos por *click* al titular del registro. *Vid.* Sunderland (2010), pág. 470. Igualmente, *vid.* Lastiri Santiago (2014) págs. 31 y ss.

[21] Clark (2003), pág. 1489.

[22] *Second Level Doman Names* o nombres de dominio de segundo nivel. Bajo un determinado dominio de primer nivel se ubica uno de segundo nivel, que permite hospedar un sitio web en la Red. Es la cadena de letras ubicada antes del TLD, y se utiliza como recurso mnemotécnico. Generalmente consiste en incorporar el nombre de la empresa o marca correspondiente. *Vid.* Baratta, O. M. y Hanaman (2000)

[23] Dhir (2008).

[24] Soler Masota (2004), págs. 20-21, nota 34.

Un caso particular del *typosquatting* es el denominado *mousetrap* (trampa para ratones), que pretende redirigir el tráfico a páginas web que alojan contenidos pornográficos. Es frecuente ver este tipo de práctica con nombres de dominio referentes a la infancia o actividades infantiles[25].

3. El *combosquatting*

Otro abuso de registro de nombres de dominio generalizado es el *combosquatting.* En esta clase de ciberocupación se registra un nombre de dominio muy similar a los que utilizan, por ejemplo, en el sector bancario, en el comercio *online* o bien en plataformas digitales. En esta práctica, las marcas registradas se unen junto con una palabra «anzuelo» que puede engañar al público consumidor sobre la procedencia u origen del mensaje, de tal forma que el usuario le resulte una dirección confiable en el momento en que comprueba en el navegador su existencia[26].

Como ejemplos podemos citar *bbva-seguro.com* o *netftlix-pagos.com*. En ocasiones se puede cambiar una letra o hacer variaciones difíciles de percibir. Estos nombres de dominio se utilizan en correos electrónicos de *phishing*, ya que permite dirigir a los usuarios a sitios webs con una dirección y apariencia muy parecida a las de los legítimos sitios web. Este tipo de *cybersquatting* es una combinación de *typosquatting* con *phishing*.

4. *Clickfarming*

El *clickfarming* se presenta cuando un nombre de dominio correspondiente a la marca o nombre personal de un tercero es utilizado para atraer a los usuarios a un sitio web que está formado predominantemente por anuncios publicitarios y obtener así ingresos a través del *Pay-per click advertising*[27].

El *clickfarming* que involucra marcas reconocidas con deliberadas faltas de ortografía es considerado como una forma de *typosquatting,* La diferencia radica en que para los *clickfarmers* el beneficio económico no deriva de la venta de un nombre de dominio, sino de su utilización para generar ingresos por medio de la publicidad insertada en el sitio web[28].

5. *Soundsquatting*

Conforme la tecnología avanza los *cybersquatters* van creando herramientas más sofisticadas para conseguir de forma fraudulenta los nombres de dominio. Este es el caso del *soundsquatting* que consiste en la ocupación ilegal del sonido. Esta usurpación se lleva a cabo utilizando una técnica que se basa en el sonido acudiendo las palabras homófonas. Estas son aquellas que suenan de la misma manera pero que se escriben de distinta forma.

---

[25] En este sentido, *vid.* Sunderland (2010). Igualmente, *vid.* caso núm. 2000-0823 *Rincón del vago, S. L. y otros vs. Nettika S.L.*, dirigido por el profesor César Giner Parreño como letrado. Este caso se abordó el problema de la redirección de la página web de Rincón del Vago al nombre de dominio *planetacondon.com* que alojaba una página web donde se comercializaban preservativos y otros productos de carácter sexual.

[26] Chen y Szurdi (2020).

[27] Lipton (2008), pág. 1481.

[28] Lipton (2010), pág. 460.

En este caso los *cybersquatters* registran variantes de palabras homófonas de nombres de dominios conocidos por los usuarios y de esta forma logran hacerse con el activo. Como ejemplos podemos citar *antenatres.es* en vez de *antena3.es, 4ever21.com* en vez de *forever21.com* o *tele5.es* en lugar de *telecinco.es*. La homofonía existe porque hay un grupo de grafemas en el castellano cuya pronunciación varía regionalmente, de tal modo que se pronuncian de forma muy similar.

En el *soundsquatting* se utilizan los homófonos en lugar de errores tipográficos y a medida que los programas de reconocimiento de voz como puede ser Alexa o Siri se vayan perfeccionando, se prevé el aumento de este tipo de ciberocupación, logrando el robo del tráfico web, estafas o ataques de *phishing*, así como llevar a los usuarios del dominio a sitios webs no deseados[29].

6. *Bitsquatting*

El *bitsquatting* es la práctica donde el *cybersquatter* se aprovecha de los errores ocasionales de hardware que son causados por un cambio aleatorio de bits en la memoria donde se almacenan temporalmente los nombres de dominio.

Los dominios tienen un carácter que difiere en un bit del mismo carácter que el dominio oficial de destino. Por ejemplo *micposoft.com* y *Microsoft.com*. Es una especie de *typosquatting* pero en bits. La ocupación de bits puede beneficiar a los atacantes porque un error de hardware puede ocasionar un cambio de bits aleatorio en la memoria donde los nombres de dominio se almacenan temporalmente. Por tanto, puede suceder que los usuarios que escriban los nombres correctamente puedan ser redirigidos a nombres de dominio maliciosos[30].

En este tipo de ciberocupación de nombre de dominio, es posible utilizar los errores aleatorios para atacar objetivos remotos a través de Internet. El *bitsquatting* se basa en esos errores aleatorios para redirigir conexiones destinadas a nombres de dominios conocidos, que son generalmente los que incorporan marcas registradas. Aquí no se requiere explotación ni ingeniería inversa complicadas. Está probado que los sitios web populares pueden redirigir cantidades nada desdeñables de tráfico de Internet a un sitio web malicioso, es decir, a un link que aparentemente es confiable, pero al hacer un click, te redirige a un sitio web falso que imita a una web oficial o legítima[31].

El *bitsquatting* es un vector de ataque real, verificado experimentalmente. En seis meses de medición, más de 16.000 computadores únicas se vieron afectadas por la ocupación de bits de varios nombres de dominio populares[32].

---

[29] Chen y Szurdi (2020).

[30] *Ibid.*

[31] El *hardware* de un ordenador puede y experimenta errores. En tecnologías de memoria, se ha estimado una tasa de error que oscila entre 3 errores por mes y 3 errores por hora por un ordenador portátil de, por ejemplo, 4 GiB. Incluso las estimaciones más bajas arrojan 600, errores por bit por día en los dispositivos informáticos del mundo. Algunos de estos errores pueden ser aprovechados por los ciberocupas donde pueden registrar nombres de dominio que sean mínimamente distintos a un nombre de dominio popular y esperan a que ocurra un error de bit aleatorio. Eventualmente, se produce el error de bit en un dispositivo en el momento y lugar adecuado para dirigir a un usuario desprevenido hacia una web no deseada. Nick Nikiforakis, Van Acker, Wannes, Desmet, Piessens y Joosen (2013).

[32] Dinaburg (2021).

7. *Cybersquatting* a través de nombres de dominio internacionalizados

Con el propósito de hacer accesible Internet a los usuarios de todo el mundo, la ICANN admitió el aumento de las opciones de nombres de dominio en todos los idiomas. Así nacieron los denominados «nombres de dominio internacionalizados» o «nombres de dominio plurilingües». Los *Internationalized Domain Names* (IDN) son nombres de dominio representados con los caracteres del idioma local. Estos nombres de dominio pueden contener caracteres con signos diacríticos (utilizados por numerosos idiomas europeos) o caracteres de códigos no latinos, tales como el árabe o el chino[33].

A este tipo de *cybersquatting* que es una variante de *typosquatting* se le denomina *homograhsquatting* porque los *cyberquatters* se aprovechan de los dominios internacionalizados, en los que se utilizan caracteres Unicode. Los atacantes suelen reemplazar uno o más caracteres en el dominio de destino con caracteres visualmente similares de otro idioma. Estos dominios son imposibles de distinguir, como es el caso de *apple.com* donde la letra inglesa «a» (U+0061) ha sido reemplazada por la letra cirílica «a» (U+0430)[34].

Siendo así las cosas, y tomando en consideración estas manifestaciones del *cybersquatting,* podemos señalar que entre los registrantes de dominios correspondientes a marcas se forman dos grupos distintos claramente definidos: 1) El grupo de los «especuladores», integrado por un conjunto de registrantes que, mediante una mínima inversión, registran nombres de dominio correspondientes a marcas ajenas con el objeto de revenderlos por un precio desproporcionadamente alto, y 2) los denominados *free riders,* registrantes que pretenden prevalerse del uso de un dominio idéntico o muy parecido a una marca o denominación ajenas de gran notoriedad con el propósito de desviar a los usuarios a sitios web maliciosos. Todo ello sin tener vinculación alguna con el legítimo titular de la marca[35].

V. LAS POLÍTICAS DE ICANN COMO FORMA DE ENFRENTAR LAS NUEVAS TENDENCIAS DEL *CYBERSQUATTING* DE NOMBRES DE DOMINIO

En enero de 2023 la *Uniform Domain Name Dispute Resolution Policy* (UDRPo Política Uniforme) cumplió veintitrés años de vida, y el número de demandas que ha tenido que tramitar, concretamente la Organización Mundial de Propiedad Intelectual (OMPI), en virtud de esta Política Uniforme alcanzó máximos históricos en el último año 2022[36]. Este incremento ha traído consigo

---

[33] *http://www.icann.org/en/topics/idn/* (visita: 10 de abril de 2023).

[34] Chen y Szurdi (2020).

[35] Agustinoy Guilayn (2002), pág. 70. Como ejemplo de este último grupo está el caso de *www.e-polo.com* que contenía una marca de la empresa norteamericana PRL USA Holdings, Inc., pero el registrante alojaba en su página web contenidos que se limitaban a describir los caballos que eran de su propiedad, y a publicar el reglamento del juego del polo, así como informaciones acerca de los caballos de polo en Argentina. El sitio web no hacía referencia alguna a prendas de vestir, muebles, ni a ninguna otra actividad comercial relacionada con la empresa que reclamaba el dominio, excepto la de los caballos de polo. *Vid.* caso OMPI núm. D2002-0108. *PRL USA Holdings, Inc. vs. Álvaro Collazo*.

[36] Solamente en OMPI, en el año 2016, se presentaron más de 3.000 demandas en virtud de la Política Uniforme, en las que intervinieron partes procedentes de cerca de 180 países y alrededor de 500 expertos de la OMPI de 65 nacionalidades. *Vid.* OMPI, «La evolución de la jurisprudencia de los nombres de do-

uniformidad y consenso en temas controvertidos y analizados por el Centro de Arbitraje y Mediación de la OMPI.

La UDRP es un procedimiento alternativo de resolución de disputas que no es judicial, ni arbitral, ni tampoco es una forma de mediación[37]. Cabe subrayar que la Política Uniforme no suspende la competencia de los tribunales nacionales. Tanto la UDRP como su Reglamento prevén expresamente tal circunstancia, encargándose este último de regular los posibles efectos de los procedimientos judiciales sobre este procedimiento[38].

La UDRP está formada por nueve artículos que establecen bajo qué condiciones se resolverán los conflictos que puedan surgir entre el registrante de un nombre de dominio y un tercero con relación al registro y uso del nombre de dominio de Internet registrado[39].

Aun cuando la mayor parte de la doctrina española que ha estudiado la Política Uniforme basa sus planteamientos en la versión en castellano de la UDRP publicada por la OMPI[40], en esta oportunidad nos apoyaremos en el texto publicado por la ICANN[41], en el entendido que es la entidad de la cual deriva la Política que examinamos.

El apartado *a)* de la cláusula 4 de la UDRP establece:

> *«a)* Conflictos aplicables. Deberá someterse a un procedimiento administrativo obligatorio en caso de que un tercero («el demandante») afirme ante el proveedor correspondiente, de conformidad con el Reglamento, lo siguiente:
>
> i) que su nombre de dominio es idéntico, o similar hasta el punto de poderlo confundir, a una marca de productos o de servicios sobre los cuales el demandante tiene derechos;
>
> ii) que usted no tiene derechos o intereses legítimos con respecto al nombre de dominio;
>
> iii) que su nombre de dominio ha sido registrado y está siendo utilizado de mala fe».

De ello, es preciso señalar que corresponderá en todo caso al demandante en el procedimiento probar que están presentes cada uno de los cuatro requerimientos arriba citados, pues, aunque se trata de tres apartados, el tercero exige por una parte, probar el registro de mala fe y, por otro, el uso de mala fe del nombre de dominio[42].

---

minio» en *https://www.wipo.int/wipo_magazine/es/2017/05/article_0008.html* (visita: 10 de abril de 2023). Además de los casos relativos a los dominios genéricos de primer nivel como el *.com*, cada vez son más frecuentes los relativos a ccTLD, como *.cn* y .中国 para China, *.eu* para la Unión Europea o *.ua* para Ucrania. OMPI, «Aumento del número de casos de ciberocupación administrados por la OMPI durante la crisis del COVID-19», en *https://www.wipo.int/amc/es/news/2020/cybersquatting_covid19.html* (visita:10 de abril de 2023); «España en el quinto puesto en demandas por ocupación de dominios en Internet», *El País*, 12 de enero de 2023, *https://cincodias.elpais.com/cincodias/2023/01/11/legal/1673454489_264779.html* (visita: 12 de abril de 2023).

[37] Vallés Botey (2002); Casas Vallés (2002), págs. 1508-1509.

[38] Cláusula 4 de la UDRP y cláusula 18 del Reglamento de la UDRP.

[39] Cláusula 1 de la UDRP.

[40] Texto disponible en *http://www.wipo.int/amc/es/domains/rules/index.html* (visita: 10 de abril de 2023).

[41] Texto disponible en *https://www.icann.org/resources/pages/udrp-2012-02-25-es* (visita: 10 de abril de 2023).

[42] Carbajo Cascón (2002), pág. 263.

Como consecuencia de la redacción de este apartado, las decisiones tomadas bajo la aplicación de la UDRP se basan generalmente en consideraciones de carácter comercial[43].

En la Política Uniforme encontramos varios elementos, los cuales, han sido objeto de diferentes interpretaciones a cargo de los expertos del Centro de Mediación y Arbitraje de la OMPI, por ello, se han establecido criterios comunes, que dicha organización llama «Jurisprudencia». Entre ese *case law* podemos encontrar cuestiones que serían aplicables a estas nuevas clases de *cybersquatting*.

1. Riesgo de confusión en la jurisprudencia de la UDRP

Las nuevas tendencias de ciberocupación las podemos calificar como distintos tipos de *typosquatting* y uno de los objetivos de esta práctica es confundir al público consumidor. Por ello, el análisis de los expertos sobre el riesgo de confusión nos puede ser de utilidad para encontrar una respuesta contundente a esta práctica maliciosa actividad.

En un principio, la identidad y similitud entre la marca y el nombre de dominio, tenía que ser valorado de acuerdo con los criterios comunes de riesgo de confusión imperantes en el Derecho de marcas[44] cuestión que dificultaba la resolución en algunos casos.

El juicio de identidad o semejanza que en ocasiones se hace bajo el auspicio de la UDRP suele ser abstracto, pues se enfoca única y exclusivamente sobre la configuración del nombre de dominio y la marca en conflicto, omitiendo la valoración acerca de la utilización o no utilización del dominio para identificar bienes o servicios y, en su caso, la comparación entre bienes o servicios iguales o similares a los de la marca cuyos derechos presuntamente vulnera[45].

La variedad de opiniones y apreciaciones, basadas generalmente en el juicio de identidad o similitud, que indican las distintas legislaciones de marcas, dio lugar a una disparidad de interpretaciones. No obstante, es ya criterio aceptado que, si la marca resulta reconocible de algún modo en el nombre de dominio, aun cuando se trate de una errata intencionada (*typosquatting*)[46] o se utilice tipografía «internacional» acentuada, los expertos dictaminarán que el nombre es similar hasta el punto de crear confusión con la marca objeto de la demanda.

---

[43] Lipton (2010), pág. 36.

[44] Martínez Medrano (2001).

[45] En este sentido, *vid.* un análisis de algunos casos en Carbajo Cascón (2002), págs. 267-268, y Agustinoy Guilayn (2002), pág. 132.

[46] El *typosquatting* es considerado como una nueva forma de *cybersquatting*. Se define como la alteración de la literalidad de la denominación de la marca con la intención de generar confusión con el signo distintivo original. Soler Masota, Paz (2004), pág. 19. Los *typosquatters* registran nombres de dominio que son premeditadas faltas de ortografía o errores en la denominación de la marca notoria o renombrada para obtener provecho de su reputación. La intención es la obtención de beneficios económicos, ya sea mediante la venta del nombre de dominio al titular del derecho de marca o el cobro de un canon por redirigir a los visitantes hacia su página web, o bien comercializando bienes o servicios, mediante publicidad, a través del parking de dominios o simplemente creando sus propias webs para generar tráfico en las mismas. Clark, Ch. (2003), pág. 1489. Un caso paradigmático de *typosquatting* fue el que enfrentó a *Shields vs. Zuccarini,* 254 F. 3d 476, 483 (3d. Cir. 2001), disponible en *http://scholar.google.com/scholar_case?case=3776366602637795017&q=Shields+v.+Zuccarini&hl=en&as_sdt=2002* (visita: 10 de abril de 2023).

Igualmente, las decisiones derivadas de la UDRP han considerado que, a efectos de evaluar la identidad o similitud entre la marca y el nombre de dominio, deben tenerse en cuenta los criterios clásicos del Derecho de marcas, tales como la comparación fonética y gráfica entre marca y dominio, así como el número de coincidencias entre ambas. Dicho criterio es utilizado para combatir también los llamados *suck cases*[47].

2. El interés legítimo en la jurisprudencia de la UDRP

Un segundo elemento que hay que tomar en cuenta para combatir la ciberocupación y que es de especial interés dadas las nuevas tendencias de esta práctica parasitaria, es que el demandante acredite que el demandado no ostenta ningún tipo de derechos o intereses legítimos respecto al nombre de dominio. En este sentido, la cláusula 4 (c) establece los criterios indicativos de la legitimidad del uso del nombre de dominio que dice:

> «c) [...] Cualquiera de las circunstancias que se exponen a continuación, entre otras, servirá como prueba de sus derechos o legítimos intereses sobre el nombre de dominio [...]:
>
> i. antes de recibir la notificación de la demanda, usted ha utilizado, o ha efectuado preparativos demostrables para utilizar el nombre de dominio o un nombre correspondiente al nombre de dominio en relación con una oferta de buena fe de productos o servicios;
>
> ii. usted (en calidad de particular, empresa u otra organización) es conocido comúnmente por el nombre de dominio, aunque no haya adquirido los derechos de marca correspondientes;
>
> iii. usted está haciendo un uso legítimo no comercial o un uso leal del nombre de dominio, sin intención de confundir a los consumidores o empañar la marca de los productos o servicios en cuestión con ánimo de lucro».

Es claro que en el caso de los tipos de *typosquatting* que acabamos de detallar, el *cyberquatter* no podrá acreditar interés legítimo. Sin embargo, es posible que pueden intentar acreditarlo bajo el concepto de libertad de expresión. En este caso, los expertos han analizado en este sentido el asunto de los nombres de dominio que contienen la palabra *suck*. Estos criterios podrían ser aplicables en los casos, por ejemplo, del *clickfarming.*

En este sentido, cabe destacar que con la entrada del nuevo nombre de dominio de primer nivel genérico (nuevo gTLD). *Sucks* en el espacio de nombres, se ha reportado el aumento de registros de nombres de dominio con la formula *marca.sucks*[48]. Entre los argumentos que utilizan esos registrantes para justificar su derecho o intereses legítimo, es demostrar que lo que hace el sitio web alojado en el dominio es en el ejercicio de la libertad de expresión. Por ello, los expertos de la UDRP, que, aunque son firmes defensores de la libertad de expresión, son conscientes que en numerosas ocasiones se recurre a este argumento para enmascarar una actividad desleal y es criterio aceptado que salvo en

---

[47] El término *suck* (que en inglés significa «apesta») se utiliza en aquellos casos en los que se añade esta palabra en los SLD que contienen marcas renombradas o notorias. Un ejemplo de estos casos, *vid.* caso OMPI D2005-0168. *Societé Air France vs. Virtual Dates, Inc*. Un análisis de este caso y otros similares, *vid.* Lipton, J. (2005), págs. 1399-1401. También, *vid.* Carbajo Cascón (2002) y Agustinoy Guilayn (2002). pág. 134.

[48] El nuevo *gTLD.sucks* entró al espacio de nombres en el año 2015.

circunstancias determinadas, un nombre de dominio que coincida exactamente con el de un titular de marca genera un riesgo de confusión, ya que puede inducir a los consumidores a creer erróneamente que dicho dominio cuenta con el respaldo de su titular.

Aunado a estos criterios, la práctica ha ido asentando otras pautas que también pueden considerarse como una ayuda para determinar si existe o no interés legítimo. Algunos panelistas han determinado que ciertas actividades recogidas, no ya en el significado de la denominación del SLD, sino en la página web, pueden ser consideradas como beneficiosas para probar el interés por parte del demandando[49].

3. El registro y uso de mala fe en la jurisprudencia de la UDRP

Otro elemento importante por tomar en consideración para paliar las nuevas tendencias de *cybersquatting*, es el registro y uso de mala fe del nombre de dominio. La mala fe es decisiva en la UDRP, pues la valoración de la misma está siempre presente, tanto para estimar la identidad o similitud entre el nombre de dominio y las marcas sobre las que puede crear confusión, siquiera en abstracto, como para apreciar el interés legítimo del titular en el nombre de dominio[50].

Las decisiones derivadas de la UDRP han interpretado ampliamente la doble exigencia de demostrar la mala fe del registrante del dominio tanto al momento de su registro como durante su posterior uso. Se considera que la tenencia pasiva de un nombre de dominio, combinada con otros factores, puede dar lugar a «mala fe» en el sentido de la UDRP[51]. Sin embargo, existen casos en los que se desestima la demanda cuando no se considera probada la mala fe en el registro, aunque se certifique la mala fe en el uso del nombre de dominio[52].

Según la UDRP:

> «Las siguientes circunstancias, entre otras, si el jurado las constata, constituirán prueba suficiente del registro y uso de mala fe de un nombre de dominio:
>
> i. circunstancias que indiquen que su objetivo primordial al registrar o adquirir el nombre de dominio era vender, alquilar o ceder de cualquier otro modo el registro de dicho nombre de dominio al demandante titular de la marca de productos o de servicios o a un competidor de dicho demandante por un valor superior a los costes directos documentados directamente relacionados con dicho nombre de dominio;
>
> ii. si usted ha registrado el nombre de dominio con el fin de evitar que el titular de la marca de los productos o servicios refleje la marca en un determinado nombre de dominio, siempre y cuando usted haya incurrido en una conducta de esa índole;
>
> iii. si su objetivo fundamental al registrar el nombre de dominio era obstaculizar la actividad comercial de un competidor; o
>
> iv. si al utilizar el nombre de dominio, usted ha intentado de manera intencionada atraer, con ánimo de lucro, a usuarios de Internet a su sitio web o a

---

[49] *Vid.* Rodríguez Delgado (2009-2010), pág. 417.

[50] Carbajo Cascón (2002), pág. 280.

[51] Agustinoy Guilayn (2002), pág. 141.

[52] Caso OMPI núm. D2011-0453. *Tribune Media Services, Inc. vs. Moniker Privacy Services, Domain Manager Ecorp.com. Inc*. Disponible en *http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2011-0453* (visita: 10 de abril de 2023).

> otro sitio en línea, creando confusión con la marca del demandante en cuanto al origen, patrocinio, afiliación o promoción de su sitio web o su sitio en línea o de un producto o servicio en su sitio web o sitio en línea».

La primera de las pautas para establecer si existe o no mala fe, es valorar si se trata del típico caso de *cybersquatting,* en el que el punto principal es la oferta de la cesión del dominio por un precio muy superior al de la tasa de registro o bien su alquiler. La segunda, valorar si implica un acto de competencia desleal —obstaculización—, que afecta concurrencialmente la posición de un tercero. Y la tercera, estudiar si la conducta del demandado da lugar a un resultado más general que implique la perturbación de la actividad comercial de un competidor[53].

Respecto a la primera, es preciso señalar que en la actualidad no basta con que se pruebe que el nombre de dominio es ofrecido por un precio más elevado al del registro. Ello se debe a que el grupo de expertos reconoce la existencia de los negocios de compraventa de nombres de dominio, que son lícitos, por lo que el demandante deberá tomar esto en cuenta a la hora de demostrar que hubo mala fe en el registro del nombre de dominio[54].

En el caso del *phishing*, el grupo de expertos del Centro de Mediación y Arbitraje de la OMPI ha sostenido que el uso de un nombre de dominio para fines distinto al alojamiento de un sitio web puede constituir mala fe. Dichos propósitos incluyen el envío de correo electrónico, suplantación de identidad (*phishing)*, robo de identidad o distribución de *malware*. En algunos de estos casos, el demandado puede albergar una versión que imita el sitio web del demandante[55].

VI. EL *UNIFORM RAPID SYSTEM (URS):* LA POLÍTICA DE LOS DENOMINADOS *NEW GENERIC TOP LEVEL DOMAINS* (NEW GTLD)

Su principal característica es bloquear el nombre de dominio objeto de la reclamación y se aplica en aquellos casos claros de *cybersquatting* (*clear cut cases*). A diferencia de la UDRP que el objetivo es recuperar el dominio y no sólo bloquearlo. Asimismo, este sistema se utiliza en los asuntos en los que estén involucrados nombres de dominio de segundo nivel registrado bajo los nuevos gTLD. Sin embargo, puede utilizarse también en cualquier gTLD.

El reclamante bajo el procedimiento URS debe demostrar, con pruebas *claras y convincentes*, cada uno de los tres elementos que a continuación se detallan[56]:

---

[53] Martínez Medrano (2001).

[54] INTA (International Trademark Association. Webminar), «Domain Name Enforcement: Present and Future»April 22th 2021.

[55] En este sentido *vid.* caso OMPI núm. D2010-1303 (*c3metrics.net*); caso OMPI núm. D2011-0600 (*dvix.com*); caso OMPI núm. D2013-1349 (*publixical.com*); caso OMPI núm. 2014-1471 (*accorhotels-booking.com*); caso OMPI núm. D2015-0324; caso OMPI núm. D2016-0364 (*bhpbilliton-hr.com*); caso OMPI núm. D2015-0645 (*magahr.info*); caso OMPI núm. d2015-1488 (*twittertour.com*); caso OMPI núm. D2015-1601 (*wwwbjswholesaleclub.com*): caso OMPI núm. D2015-2034 (*tetrapak-uk.com*); caso OMPI núm. D2016-0367; caso OMPI núm. D2016-0367 (*accenturejobs.com*); caso OMPI núm. D2016-0384 (*minerva-food.com*): caso OMPI nºD2016-0385 (*minecvafoos.com*); caso OMPI núm. D2016-0461(*helplineyahoo.com*); caso OMPI núm. D2016-2213 (*arlafoods.com*). El más reciente es el caso OMPI núm. 2021-0013.

[56] *Vid.* 1.2.6 del URS.

1) que el nombre de dominio es idéntico o similar hasta el punto de crear confusión con respecto a la marca de la cual es titular[57],

2) que tiene un registro nacional o regional válido y en vigor, o bien que la marca de la cual es titular ha sido reconocida a través de un procedimiento judicial o está debidamente protegida por una ley o tratado vigente al momento de la presentación de la reclamación bajo el URS, además

3) tendrá que acreditar que el registrante no tiene ningún derecho o interés legítimo respecto al nombre de dominio[58] y que este ha sido registrado y utilizado de mala fe[59].

Entre las pruebas de registro y utilización de mala fe, el URS reproduce lo establecido en la UDRP.

Pese que a que encontramos similitudes sustantivas entre la URS y la Política Uniforme, este nuevo mecanismo protector de los derechos de marca en el DNS establece nuevas medidas que pueden paliar las nuevas prácticas parasitarias del *cybersquatting.*

Una de ellas es que la URS establece que, con el propósito de demostrar la buena fe en el uso del nombre de dominio por parte del registrante demandado, el examinador podrá tomar en cuenta que la compra y venta de nombres de dominio y contar con una amplia «cartera» o serie de registros de nombres de dominio no constituyen en sí mismos indicios de mala fe. No obstante, tal comportamiento puede ser abusivo, dependiendo de las circunstancias de la controversia. El examinador deberá analizar cada caso concreto[60]. Lo anterior, revela la licitud de la venta de los nombres de dominio, siempre y cuando el examinador lo considere de esa forma. El factor de venta requerirá la característica maliciosa para que pueda considerarse *cybersquatting* bajo la URS.

Otra medida interesante es que este sistema de suspensión rápida indica que la venta de tráfico (es decir, conectar los nombres de dominio a las páginas de publicidad para obtener ganancias mediante el pago por *click*) no constituye mala fe en sí misma. Sin embargo, tal comportamiento puede ser abusivo en un caso determinado dependiendo de las circunstancias de la controversia. En este caso, el examinador deberá tener en cuenta: a) la naturaleza del nombre de dominio, b) la naturaleza de los enlaces publicitarios en la página asociada con el nombre de dominio y c) que el uso del nombre de dominio sea en última instancia responsabilidad del registrante[61].

En este punto, es preciso resaltar que para presentar una reclamación bajo la URS, es necesario tener inscrita la marca en la denominada Trademark Clearing House, lo que supone una mayor seguridad para los titulares de marca, pues esta Clearing House brinda los servicios de fase preferencial de registro y la *claim alerts*[62]. Igualmente, una reclamación bajo el URS debe incluir una prueba de uso de la marca, que puede consistir en una declaración de ese uso en el comer-

---

[57] Regla 1.2.6.1 del URS.
[58] Regla 1.2.6.2 del URS.
[59] Regla 1.2.6.3 del URS.
[60] Regla 5.9.1.
[61] Reglas 5.9.2.1 a 5.9.2.3.
[62] ICANN, «What is the Trademark Clearinghouse», *http://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs* (visita: 10 de abril de 2023).

cio junto con una muestra o ejemplo de ello. Dicha prueba debe ser certificada y validada por la *Clearinghouse.*

Es indudable la gran ventaja que representa poder bloquear los nombres de dominio de aquellos *cybersquatters* que aprovechando la evolución de las tecnologías registran marcas como nombres de dominio. No obstante, los titulares de marca deben estar atentos a las posibles apropiaciones indebidas de sus dominios a través de las nuevas tendencias de la cibeocupación, que, sin duda alguna, a medida que la tecnología evolucione con ella los registros de nombres de dominio que vulneran los derechos de marca.

Pese al crecimiento de la ciberocupación, podemos afirmar que con las actuales políticas de ICANN, los titulares de marca pueden combatir las distintas formas de *cybersquatting*. Igualmente, en el caso que las políticas de ICANN no sean suficientes podemos considerar como alternativas para combatir el *cybersquatting* del siglo XXI el derecho represor de la competencia desleal.

VII. EL *CYBERQUATTING* EN EL METAVERSO: *CRIPTOSQUATTING*

La ciberocupación en el Metaverso más que tratarse de una nueva clase de esta práctica maliciosa, se trata de la ciberocupación tal y como la entendemos, pero con un novedoso tipo de nombres de dominio.

Quizá estemos asistiendo a la transformación más significativa de este activo digital. Esto es así porque se trata de nombres nacidos y creados en la web 3.0 que son registrados en una red criptográfica, como, por ejemplo, Ethereum. Estos «nombres» que podrían ser los homólogos de los nombres de dominio de primer nivel genéricos (gTLD) no están vinculados a ninguna dirección IP ni tampoco son asignados por ICANN.

Un nombre de dominio web 3.0 se utiliza para enviar y recibir pagos en criptomonedas, acceder a dApps[63] e interactuar con *Smart Contracts*. Las direcciones criptográficas son cadenas de caracteres largas y complejas y por ello son sustituidas por nombres fáciles de recordar.

1. La Internet del metaverso

El Metaverso es un concepto web 3.0 de próxima generación que pretende complementar y potencialmente reemplazar el actual Internet web 2.0 que utilizamos en el día a día. La web 3.0 es considerada como el futuro de Internet, siendo los usuarios tanto creadores de contenido como beneficiarios del mismo[64]. Esta versión web promete la descentralización y desintermediación, es decir, la desaparición de los intermediarios que facilitan Internet, a diferencia de la web 2.0 que son los intermediarios parte fundamental del funcionamiento del mercado virtual tal y como lo conocemos.

---

[63] Las dApps o aplicaciones descentralizadas que funcionan en base a una red descentralizada de ordenadores. Los datos generados por esta aplicación están alojados en una red de ordenadores que permite que esta información se mantenga segura y accesible. Esta red descentralizada, está basada generalmente en tecnología blockchain. SÁEZ HURTADO (2022).

[64] KURT (2022).

La web 3.0 es sinónimo de un movimiento de rechazo a la centralización creciente de Internet. Las aplicaciones en web 3.0 ya no se ejecutan en un servidor, lo hacen de manera descentralizada en una red estable y fiable de miles de nodos, es decir, las aplicaciones son secundarias y los que juegan un rol primordial son los creadores de contenido. Así, los operadores de nodos, los desarrolladores de aplicaciones y los creadores de contenido alienan sus intereses y ven recompensadas sus aspiraciones gracias a la tecnología subyacente que permite repartir los incentivos necesarios para mantener la red sin entidades centrales y en este punto la *blockchain* hace posible esa descentralización[65].

¿Es el Metaverso realmente una web 3.0? Si no, ¿cuál es la diferencia entre ambas? La opinión predominante es que los dos conceptos son diferentes. En primer lugar, la web 3.0 se centra más en quién posee y controla el contenido de Internet. No obstante, el Metaverso se centra en cómo los usuarios experimentan Internet[66]. El Metaverso puede definirse como el entorno inmersivo, donde los usuarios no sólo ven un mundo virtual tridimensional, sino que están en ese entorno, representados por sus avatares. En segundo lugar, el Metaverso puede ser centralizado o descentralizado. Sin embargo, la web 3.0 se considera descentralizada y basada en *blockchain,* lo que otorga a los usuarios control sobre sus datos.

2. Los nombres de dominio tradicionales

Recordemos que Internet dio sus primeros pasos en la década de los años sesenta. Se trataba de una red, denominada Arpanet[67], que se circunscribía a la conexión de varios ordenadores pertenecientes a departamentos de investigación informática de distintas universidades norteamericanas. Dicha red no utilizaba el nombre de dominio para identificar los ordenadores que la conformaban, sino que empleaba largas direcciones numéricas para reconocer a cada usuario. Así, cada dirección numérica correspondía a un equipo o dispositivo conectado a la red.

Fue más adelante cuando Jon Postel[68], un investigador involucrado en el desarrollo de Arpanet, se dio cuenta de que los «nombres» funcionarían mejor

---

[65] Vicente del Olmo (2022), pág. 43. Igualmente, se habla ya de la Internet del futuro que es la web 4.0 que se puede considerar como un ultra-inteligente agente electrónico. Se proyecta como una web simbiótica y universal. En esta versión web la interacción entre humanos y máquinas en simbiosis se conceptualiza tan potente como el cerebro humano. Significa el progreso en el desarrollo de las telecomunicaciones, el avance de la nanotecnología en el mundo e interfaces controladas mediante la web 4.0. Se busca el paralelismo con el cerebro humano que implica una red masiva de interacciones altamente inteligentes. Fowler y Rodd (2013).

[66] PixelPlex Team, «Decentralized Economy —the Role of Blockchain in the Metaerse», 10 de febrero de 2022, *https://pixelplex.io/blog/importance-of-blockchain-in-metaverse/* (visita: 10 de abril de 2023).

[67] Arpanet (la antecesora de Internet, primera red que conectó el primer ordenador *host* a otro) contaba con más de 300 ordenadores y se había convertido en un valioso recurso para sus usuarios. La Arpanet original se dividió en dos partes: la primera se siguió llamando Arpanet, dedicada única y exclusivamente al desarrollo y la investigación, mientras que la segunda se llamó Milnet, que hacía referencia a una red militar no clasificada. La transición del protocolo para *host* de Arpanet desde un protocolo NCP (Network Control Protocol) a TCP/IP implicó un cambio muy delicado, que requería que todos los hosts se convirtieran simultáneamente o que permanecieran comunicados mediante mecanismos desarrollados para tal propósito. La conversión se llevó a cabo el 1 de enero de 1983, y la operación fue dirigida por Dan Lynch, que se considera el encargado de convertir Arpanet en Internet. A raíz de dicha conversión, muchos fabricantes incorporaron TCP/IP a sus productos. *Vid.* en este sentido Aroche (2006). Para más información sobre esta transformación, *vid.* Delgado Kloos y García Rubio (2001), pág. 25, y de Miguel Asencio, P. (2002), pág. 25.

[68] Estudiante y posteriormente científico en la University of California, Los Angeles. Fue miembro de la Internet Society (en adelante, ISOC), de la Internet Arquitecture Board (en adelante, IAB) y de la Internet

que los números y que una estructura escalonada podría ser útil para favorecer la localización e identificación de los equipos que integraban dicha red.

En el 1971, Postel propuso la utilización de ocho nombres, que correspondían a los diferentes campus de la University of California, Los Angeles (UCLA). La idea de emplear nombres en vez de números continuó desarrollándose, y en el 1982 ya se contaba con más de 400 nombres en pleno uso. Cabe recordar en este punto que en aquella época los nombres correspondían únicamente a las distintas universidades o departamentos de investigación de Estados Unidos[69]; con ellos se creó una lista de nombres y direcciones que era administrada por la Internet Assigned Numbers Authority (en adelante, IANA).

Más tarde, en 1983, Postel propuso una estructura basada en nombres de dominio de diferentes niveles: primer nivel, subnivel, etc. El primer dominio de primer nivel que existió fue *.arpa*[70].

En definitiva, los nombres de dominio tradicionales son un nombre sencillo y fácil de recordar asociado a una dirección IP, esta es una serie de números que identifica de manera lógica y jerárquica a una interfaz en red, es decir, a un ordenador que utilice este protocolo IP.

Los nombres de dominio del metaverso nacen de una forma muy similar a los nombres de dominio tradicionales, ya que las direcciones criptográficas son cadenas de caracteres largas y complejas. Por ello, los nombres fáciles de recordar eliminan esta complejidad y permiten una experiencia más fluida en la web 3.0. Al igual que los dominios de la web 2.0, los nombres de dominio del metaverso generalmente terminan con extensiones de «primer nivel», como ejemplo, *.eth, .crypto* o *.nft*.

3. Los nombres de dominio de la web 3.0: del metaverso

El nombre de dominio web 3.0 o *blockchain* puede utilizarse de varias formas dentro del ecosistema de la web 3.0. Principalmente se usa como un *friendly name* para recordar la larga y farragosa dirección criptográfica. De ese modo, el usuario puede enviar y recibir de forma más sencilla pagos en criptomonedas, acceder a dApps e interactuar con contratos inteligentes.

Las direcciones *crypto* (*bitcoin*, *ether* u otra *crypto*) son el medio principal para recibir y enviar fondos de activos digitales (criptomonedas) en una red *blockchain*. Estas direcciones son una cadena de caracteres que identifica de manera única la fuente o el destino de una transacción. Cada *blockchain* tiene direcciones de *wallets* que se crean por una operación criptográfica en un ordenador[71].

En el espacio cripto, todavía se utilizan largas direcciones (incluso más extensas que las direcciones IP) que son poco adaptables para los usuarios. Un ejemplo de dirección ETH es 0xd0eAf74B8c5bF457C7a81c3f3277aDb6Ed32DCF4,

---

Engineering Task Force (en adelante, IETF). *Vid.* Internet Society, «A ten year tribute to Jon Postel», *http://www.isoc.org/awards/postel/memory.shtml.*

[69] Consúltese en este sentido Agin (2008).

[70] *Vid.* IANA, «.ARPA Zone Management», *http://www.iana.org/domains/arpa* (visita: 10 de abril de 2023).

[71] BYB-T Learn, «Dirección de blockchain» , *Glossary*, 13 de diciembre de 2020, en *https://learn.bybit.com/es/glossary/definition-blockchain-address/* (visita: 10 de abril de 2023).

dicha cadena de 42 caracteres es difícil de memorizar. Por ello, se acudió nuevamente a los nombres y en este ámbito se recurrió a nuevos protocolos, como puede ser el ENS.

El *Ethereum Name Service* (ENS) es un protocolo utilizado para asociar nombres fáciles de recordar a direcciones de activos digitales. El proceso es similar al del *Domain Name System* (DNS).

El ENS ofrece una forma segura y descentralizada de gestionar «dominios» de sitios web y enviar *tokens* ETH y ERC20[72]. Es un servicio distribuido de código abierto que interacciona directamente con la red Ethereum. Genera nombres de dominios tipo *bbva.eth*, que son más sencillos para los usuarios. La personalización de las direcciones ENS es una opción que permite una gestión de fondos mucho más fluida.

Estos nombres de dominio del metaverso además de ser la «máscara» de las direcciones criptográficas son importantes porque reducen el riesgo en el momento de hacer transacciones con criptomonedas. Esto es así, porque un error al teclear la dirección criptográfica es irreversible. El riesgo de cometer una equivocación al gestionar los fondos en criptomonedas es alto, ya que podrían llegar a otra dirección y perderse para siempre. Por lo anterior, el objetivo principal del ENS es minimizar el riesgo para que las transacciones sean seguras. Estos nombres de dominio se pueden registrar en ENS[73].

En el metaverso también están los nombres de dominio UD (Unstoppable domains)[74]. UD son un tipo de nombres de dominio que utiliza la tecnología *blockchain*, que usan un servicio denominado Crypto Name Service que también es distinto al DNS. Pueden servir para distintas funcionalidades y una de las más comunes es la personalización de *wallets*. Así, en vez de tener una serie de caracteres se puede tener un nombre corto y fácil de recordar. Posee una filosofía distinta al ENS, pues está pensado para las empresas, ya que permite crear sitios web descentralizados donde se conectan a una especie *hosting* que permite el intercambio y distribución descentralizada de la información[75].

4. El *cybersquatting* en la web 3.0

En el siglo XXI, los *cybersquatters* están apostando por los nombres de dominio *blockchain* que incorporan marcas renombradas o notoriamente conocidas[76]. Ello se debe a la naturaleza descentralizada de los mismos. Esta ciberocupación va en aumento y con ello nace una problemática jurídica importante, ya que, a diferencia de lo que sucede con DNS donde ICANN ofrece instrumentos que son centralizadas e uniformes para paliar el problema de esta práctica nociva, los nombres de dominio del metaverso no poseen políticas de ningún tipo ni tampoco mecanismos de resolución de conflictos en materia de nombres de dominio.

---

[72] TRAN y BENSON (2022).

[73] ENS, *https://ens.domains/es/* (visita: 12 de abril de 2023).

[74] *Vid. Unstoppable domains* en *https://unstoplebedomain.net/?gclid=CjwKCAjwrdmhBhBBEiwA4Hx5g1bJdkpxDnjgQeP9lqrK6nQY5W3RWz3f_yV5x_nsaNBK4cN2K53LzhoC_VEQAvD_BwE* (visita: 12 de abril de 2023), y *Brave-help Center,* «What are Web3 domains?», *https://support.brave.com/hc/en-us/articles/13786985737229-What-are-Web3-Domains-* (visita: 10 de abril de 2023).

[75] *Ibid.*

[76] El nombre de dominio *adele.eth* se vendió por 60.000 dólares en Open Sea.

Por ejemplo, UD informa que no tiene posibilidad de recuperar el nombre de dominio una vez que este haya sido comprado o acuñado. Lo anterior, quiere decir que cuando un ciberocupa se hace con un dominio del metaverso que incorpora una marca, el titular de esta, no tiene un mecanismo de resolución comparable con la Política uniforme de resolución de disputas (UDRP) para recuperar el dominio o bien un URS para bloquear el dominio en el metaverso.

Esta falta de instrumentos jurídicos o políticas concernientes a nombres de dominio, ha atraído la atención de los *cybersquatters*. Esta práctica parasitaria sería fácil de abordar a través de la UDRP en el caso de un nombre de dominio tradicional, pero dado que no existe una política comparable para dominios de metaverso descentralizados, los titulares de marcas se encuentran en una especie de limbo jurídico.

Por lo anterior, los titulares de marca deben considerar el registro de sus marcas como nombres de dominio *blockchain*. Ello, es importante porque además de constituir registros defensivos, permitirían pagos criptográficos para sus bienes y servicios. Nike, por ejemplo, registró extensiones como *.eth .crypto, .nft, .wallet,* entre otros, lo que posibilitaría a los visitantes de Nikeland comprar productos con criptomonedas[77].

Nuestro estudio excedería de los límites marcados por el espacio que se nos concede si nos extendiéramos a considerar en toda su amplitud la cuestión compleja que presentan estos nombres de dominio del metaverso. No obstante, podemos mencionar dos estrategias que pueden plantearse los titulares de marca. La primera, es que los titulares pueden luchar contra los *cybersquatters* en los metaversos centralizados (Roblox) o en los *e-markets* (OpenSea) que disponen de procedimientos para hacer frente a las violaciones de los derechos de propiedad intelectual en sentido amplio. La segunda, es que en países como EE.UU.A, que cuentan con la *Anticybersquatting Consumer Protection Act* (ACPA) se establece la acción *in rem* que sugiere el tratamiento del nombre de dominio como bien jurídico material y la evaluación del potencial valor económico de los nombres de dominio. Lo anterior, trae consigo la posibilidad de poder recuperar un nombre de dominio[78].No obstante, hay que recordar el carácter descentralizado de esto cripto nombres de dominio. Con ello, se nos presenta un verdadero galimatías jurídico que de no resolverse en un tiempo relativamente corto, sólo beneficiará a los *cybersquatter*[79].

VIII. BIBLIOGRAFÍA

Agin, Warren (2008), «Domain Names as Collateral. Are We All Just Kidding Ourselves?», *Business Law Today,* American Bar Association, 1, septiembre-octubre, *http://www.abanet.org/buslaw/blt/2008-09-10/agin.shtml* (visita: 10 de abril de 2023).

Agustinoy Guilayn, Albert (2002), *Régimen jurídico de los nombres de dominio.* Tirant lo Blanch, Valencia.

Aroche, Sthepanie (2006), «Historia de Internet», *http://www.maestrosdelweb.com/editorial/internethis* (visita: 10 de abril de 2010).

---

[77] *Vid.* Torrejón (2022).

[78] En este sentido, *vid.* Agin (2008).

[79] De Maere (2022). Además, *vid.* Jayaram (2022).

Callmann, Rudolph (1981), *The Law of Unfair Competition Trademarks and Monopolies,* 4.ª ed., Clark Boardman Callaghan, New York.
Carbajo Cascón, Fernando (2002), *Conflicto entre signos distintivos y nombres de dominio en Internet,* 2.ª ed., Aranzadi, Pamplona.
Casas Vallés, Ramón (2002), «Política uniforme para la resolución de conflictos en materia de nombres de dominio», en Cremades, J.; Fernández-Ordóñez, M. A., e Illescas Ortiz, R. (coords.), *Régimen jurídico de Internet,* Madrid, págs. 1495-1072.
Clark, Christopher (2004), «The Truth Domain Names Act Of 2003 and a Preventative Measure to combat Typosquatting», 89 *Cornell L. Rev.,* págs. 1477-1518.
Chen, Zhanhao, y Szurdi, Jane (2020), «Cybersquatting: Attackers Mimichking domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers», *Unit 42,* 1 de septiembre, *https://unit42.paloaltonetworks.com/cybersquatting/* (visita: 10 de abril de 2023).
De Maere, Jenes (2022), «Metaverse domains: both virtue and vice for trademarks owners», *Lexology,* 19 de diciembre, en *https://www.gevers.eu/blog/trademarks/metaverse-domains-both-a-virtue-and-a-vice-for-trademarks-owners/* (visita: 10 de abril de 2023).
De Miguel Asensio, Pedro Alberto (2002), *Derecho privado de Internet,* Civitas, Madrid.
Delgado Kloos, Carlos, y García Rubio, Carlos (2002), «Historia de Internet», en Cremades, J.; Fernández-Ordóñez, M. A., e Illescas Ortiz, R. (coords.), *Régimen jurídico de Internet,* La Ley, Madrid, págs. 87-111.
Dhir, Reshika (2008), «Typosquatting a civil conspirancy», *IP Osgoode,* 9 de noviembre, *http://www.iposgoode.ca/2008/11/typosquatting-a-civil-conspiracy* (visita: 10 de abril de 2023).
Dinaburg. Artem (2021), «Bitsquatting. DNS Hijacking without Explotation», *Rayton Company*, julio, *https://media.blackhat.com/bh-us-11/Dinaburg/BH_US_11_Dinaburg_Bitsquatting_WP.pdf* (visita: 10 de abril de 2023).
Flinn, Patrick. J. (2008), *Handbook of Intellectual Property Claims and Remedies New York,* Gaithersburg, Aspen Law & Business.
Fowler, Jonnathan, y Rodd, Elizabeth (2013), «Web 4.0: The Ultra-Intelligent Electronica Agent is Coming», 27 de marzo, *https://bigthink.com/articles/web-40-the-ultra-intelligent-electronic-agent-is-coming* (visita: 10 de abril de 2023).
Gilwit, Dara (2003), «The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How To Prevent Public Deception and Trademark Infringement», 11 *Wash. U. J. L. & Pol'y,* págs. 267-296.
Gilson, Jeremy, y Gilson, Ann (2005), *Cinnamon Buns, Marching Ducks, and Cherry-Scented Racecar Exhaust: Protecting Nontraditional Trademarks,* Lexis Nexis, Matthew Bender, New York.
Gilson, Jeremy, y Samuels, Mathew (2003), *Trade-mark Protection and Practice,* Matthew Bender, New York.
Herrador Muñoz, Manuel (2014), «Plan del proyecto. Servicios de internet orientados a los negocios», *Escuela Politécnica Superior de Jaén, https://sinbad2.ujaen.es/sites/default/files/publications/pfc_manuel_herrador.pdf* (visita: 10 de abril de 2023).
Jayaram, Vivek (2022), «La Web3 Ya sufre de Ciberocupacion o Cybersquatting: Que Pueden hacer las marcas?», *Decrypt,* 6 de julio, *https://decrypt.co/es/104482/la-web3-ya-sufre-de-ciberocupacion-o-cybersquatting-que-pueden-hacer-las-marcas* (visita: 10 de abril de 2023).
Kurt, Ivy (2022), «From Web. 2.0 to Web. 3.0» How these Entrepreneurs Made the Swicht, *Entrepeneur,* 8 de junio, *https://www.entrepreneur.com/money-finance/from-web-20-to-web-30-how-these-entrepreneurs-made-the/427019* (visita: 10 de abril de 2023).
Martínez Medrano, Gabriel (2001), «Los nombres de dominio en Internet. Sistema mundial de solución de controversias», *http://www.dominiuris.com/boletines/doctrinal/gabriel2.htm#_ftnref4* (visita: 10 de abril de 2023).

McCarthy, Thomas (1997), *Trademarks and Unfair Competition,* 4.ª ed., Clark Boardman Callaghan, New York.
Massaguer Fuentes, José (1998), «Conflicto de marcas en Internet», *Revista General de Derecho,* núm. 648 (1997), págs. 11107-11142.
Mihai, Ioan Cosmin (2012), «Overview on Phishing Attacks», *1 Int'l j. Info. Sec. & Cybercrime,* vol. I, núm. 2, págs. 61-67.
Nelmark, David (2004-2005), «Virtual Property: The Challenges of Regulating Intangible, Exclusionary Property Interest Such as Domain Names», 3 *Nw. J. Tech. & Intell. Prop.,* págs. 1-23.
Nikiforakis, Nick; Van Acker, Steven; Wannes Meert †; Desmet, Liven; Piessens, Frank, y Joosen, Wouter (2013), «Belgium. "Bitsquatting: Exploiting Bit-Flips for Fun, or Profit?"», *https://www.securitee.org/files/bitsquatting_www2013.pdf* (visita: 10 de abril de 2023).
Lastiri Santiago, Mónica (2014), *La comercialización del nombre de dominio. Régimen jurídico,* Marcial Pons, Madrid.
Lipton, Jacqueline (2005), «Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy», 40, *Wake Forest L. Rev.*, págs. 1361-1440.
— (2008), «Celebrity in Cyberspace: A Personality Rights Paradigm for Personal Domain Name Disputes», 65 *Wash & Lee L. Rev.*, págs. 1445-1528.
— (2010), «Bad Faith Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution», *Harvard Journal of Law & Technology,* vol. 23, 2, págs. 447-481.
Lipton, Jacqueline, y Brennan, David (2010), *Internet Domain Names, Trademarks and Free speech,* Center for Intellectual Property Law and Technology, University of Akron School of Law, US.
Ramos Herranz, Isabel (2004), *Marcas versus nombres de dominio,* Iustel, Madrid.
Rodríguez Delgado, Juan Pablo (2009-2010), «Resolución de controversias en materia de nombres de dominio a la luz de los criterios utilizados por los panelistas de la OMPI (Especial referencia a las resoluciones dictadas por los expertos españoles)», *ADI* 30, págs. 405-435.
Sáez Hurtado, Javier (2022), «Qué don las dApps o aplicaciones descentralizadas y varios ejemplos», *IEBS. Finanzas,* 25 de febrero, *https://www.iebschool.com/blog/dapps-o-aplicaciones-descentralizadas-que-son-y-como-funcionan-finanzas/* (visita: 10 de abril de 2023).
Sammarco, Pieremilio (2002), *Il regime giuridico dei 'nomi a dominio,* Giuffrè Editore, Milán.
Sanz de Acedo Hecquet, Etienne (2001), *Marcas renombradas y nombres de dominio en Internet: en torno a la ciberpiratería,* Civitas, Madrid.
Soler Masota, Paz (2004), «Conflictos sobre nombres de dominio: últimas tendencias en las decisiones OMPI», *Pe i Revista de Propiedad Intelectual,* 17, Madrid, págs. 11-30.
Slavin, Kelly (2004), «Protecting Your Intellectual Property from Domain Name», *FindLaw, https://corporate.findlaw.com/intellectual-property/protecting-your-intellectual-property-from-domain-name.html* (visita: 10 de abril de 2023).
Sunderland, Sara (2020), «Domain Name Speculation: Are We Playing Whac-a Mole?», 25 *Berkeley Tech. L. J.*, págs. 465-490.
Torrejón, Manuel (2022), «Nike sigue comprando dominios dentro de la Red Ethereum», *Bitcoin.es,* 31 de mayo, *https://bitcoin.es/actualidad/nike-sigue-comprando-dominios-dentro-de-la-red-ethereum/* (visita: 12 de abril de 2023).
Tran, Ki Chon, y Benson, Jeff (2022), «¿Qué es el servicio de nombres de dominio de Ethereum (ENS)?», *Decrypt,* 20 de febrero, *https://decrypt.co/es/resources/que-es-servicio-de-nombres-de-ethereum-ens* (visita: 10 de abril de 2023).
Vallés Botey, Martí (2002), «El proceso cuasi-arbitral en conflictos relativos a nombres de dominio», *Anuario Justicia Alternativa,* 2, *http://vlex.com/vid/cuasi-arbitral-conflictos-relativos-nombres-246941* (visita: 10 de abril de 2023).