UN ANÁLISIS DE LOS PROCESOS DE RESOLUCIÓN DE LITIGIOS SOBRE CONTRATOS ILÍCITOS EN LOS MERCADOS DE LA RED OSCURA*

AN ANALYSIS OF THE DISPUTE RESOLUTION PROCESSES FOR ILLICIT CONTRACTS IN DARK WEB MARKETS

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 70-103

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033. El autor agradece los comentarios aportados al borrador inicial por la Dra Ana Montesinos García y el Dr Norberto Redondo Melchor. Naturalmente, cualquier posible error en el texto es responsabilidad exclusiva del autor.

Pablo CORTÉS

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Este artículo explora cómo los participantes en los mercados de la Red Oscura acceden a herramientas para evitar disputas y sistemas para resolverlas, diseñados para minimizar y resolver disputas surgidas de transacciones ilícitas. Un número creciente de personas recurre a la Dark Web para realizar actividades principalmente ilegales, que incluyen la compra de drogas, la adquisición de ransomware y armas. Los pagos generalmente se realizan a través de un sistema de depósito en garantía ("escrow") que retiene la criptomoneda pagada por compradores anónimos a vendedores anónimos hasta que los compradores confirman su satisfacción con la transacción. Cuando los compradores no están satisfechos y no pueden resolver su queja directamente con el vendedor, pueden iniciar una disputa en la cual típicamente un adjudicador independiente congela el pago depositado y considera las pruebas proporcionadas por las partes, y a menudo también las opiniones de la comunidad del mercado, y determina el resultado de la disputa. El artículo analiza las herramientas y sistemas diseñados para evitar y resolver disputas, cuyo objetivo es fortalecer la confianza en transacciones ilícitas anónimas en los mercados oscuros. Se argumenta que la implementación de estos mecanismos de resolución de disputas están fomentando el desarrollo orgánico de un ecosistema de justicia civil dentro de la Red Oscura.

PALABRAS CLAVE: Resolución Alternativa de Litigios; red oscura; prevención de litigios; arbitraje; mediación.

ABSTRACT: *This paper seeks to unravel how participants in the marketplaces of the Dark Web have access to dispute avoidance tools and dispute resolution systems designed to minimise and settle disputes arising from illicit transactions. A growing number of individuals go the Dark Web to carry out mostly illegal activities, which range from the purchase of illegal drugs to the purchase of ransomware and weapons. Payments typically take place via an escrow system that holds the cryptocurrency paid by anonymous buyers to anonymous sellers until the buyers confirm their satisfaction with the transaction. When buyers are not satisfied and cannot settle their complaint directly with the seller, they can start a dispute whereby typically an independent adjudicator freezes the payment in the escrow and considers the evidence provided by the parties, and often also the views of the marketplace community, and determines the outcome of the dispute. The paper examines the dispute avoidance and resolution tools that seek to enhance trust in anonymous peer to peer illicit transactions, and it argues that these emerging dispute resolution systems are contributing to the organic growth of a civil justice ecosystem for the Dark Web.*

KEY WORDS: *Alternative dispute resolution; dark web; dispute prevention; arbitration; mediation.*

I. INTRODUCCIÓN.

La Red Oscura, conocida también como la *Dark Web* o la *Dark Net*, es la parte de Internet no indexada por los buscadores tradicionales como Google. Sólo es accesible a través de un software especializado, como TOR, que encripta la información y la ubicación de sus usuarios, lo que la convierte en un refugio seguro para la transacción de bienes y servicios ilegales, como drogas, bienes robados, armas, pasaportes falsificados y ransomware,[1] así como servicios, desde campañas de spam, hasta asesinatos por encargo. La combinación de la creciente actividad de la red TOR y el avance de la tecnología de las criptomonedas que también garantizan el anonimato del usuario, ha desempeñado un papel importante en el auge de un comercio ilícito fuera del alcance de las fuerzas del orden público.

Aunque los mercados en la Dark Web operan en un ámbito no regulado, en muchos aspectos funcionan como mercados en línea tradicionales como eBay o Amazon. Sin embargo, a diferencia de Amazon, los administradores del mercado normalmente no venden directamente a los clientes, sino que simplemente ofrecen un espacio virtual para que compradores y vendedores realicen transacciones; y a diferencia de eBay, no hay subastas, ya que todos los artículos a la venta normalmente tienen un precio fijo. Como el número de estas transacciones, al igual que las del comercio electrónico legal, ha aumentado en los últimos años,[2] también ha surgido la necesidad de usar algún tipo de mecanismo de resolución de litigios. Actualmente, la mayoría de los mercados de la Dark Web ofrecen un sistema de reclamación y de resolución de litigios.[3] Además, los mercados más

1 Los ataques de ransomware consisten en la encriptación de los datos del ordenador y la red de la víctima y exigen cripto pagos a través de la Dark Web para mantener el anonimato de los piratas informáticos. Véase Vanian, J.: 'Online criminals have created their pseudo court system on the dark web' *Fortune* (7 diciembre 2021). Véase https://fortune.com/2021/12/07/online-criminals-court-system-dark-web-russian-hackers-ransomware/. En adelante, última vez accedido el 3 de abril de 2024

2 United Nations Office on Drugs and Crime, Global Overview – Drug Demand Drug Supply, Global Drug Report 2022. p. 58. Véase https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_2.pdf.

3 Holland, A. et al.,: 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back' An HP Wolf Security Report' 2022, pp. 4 y 15. Véase https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf

• Pablo Cortés
Catedrático Leicester School of Law, University of Leicester (Reino Unido), pablo.cortes@le.ac.uk

grandes del Dark Net tienen miles de usuarios a los que ofrecen un servicio de atención al cliente 24 horas al día, 7 días a la semana.

El pago de las actividades comerciales en la Dark Web se realiza mediante criptomonedas a las que su posible anonimato del usuario permite referirse a ellas como el efectivo digital. Estos cripto-pagos también facilitan la auto-ejecución de las decisiones porque normalmente se entregan a través de un depósito en garantía (llamado servicio de custodia o *escrow*) que retiene el monto de la transacción hasta que el comprador confirma que está satisfecho con la transacción (o hasta que ha pasado el período de tiempo establecido).[4] Si una de las partes no está satisfecha con la transacción, puede iniciar una reclamación que a menudo se resuelve con la asistencia del administrador del mercado que controla el depósito de la transacción.

Por lo tanto, cada vez hay más procesos de resolución de litigios en línea que se emplean habitualmente para resolver disputas entre compradores y vendedores de acuerdo con las normas específicas de cada mercado de la Dark Web y con las condiciones generales de venta acordadas por las partes. Estos procesos frecuentemente aseguran la ejecución de la decisión, no solo a través del sistema de depósito del servicio de custodia (*escrow*), sino también a través del uso de incentivos (ej., la reputación del vendedor se verá afectada por un comentario negativo del comprador) y sanciones (ej., la expulsión de usuarios del mercado), pues es crucial garantizar el cumplimiento extrajudicial de la decisión, ya que naturalmente las partes no pueden acudir a los tribunales nacionales para hacer cumplir el resultado de litigios relacionados con transacciones ilegales. El objetivo de estas herramientas de prevención y resolución de litigios no es otro que aumentar la confianza entre los usuarios que participan en el comercio ilícito, reduciendo al mismo tiempo el riesgo de represalias por parte de las víctimas de transacciones fraudulentas o controvertidas.

A pesar de la existencia de estos sistemas de resolución de disputas, hay una escasez de información disponible sobre estos procesos porque los mercados en la Dark Web no han sido ampliamente estudiados dada la dificultad para acceder a ellos, el anonimato de los usuarios, y los riesgos que implica navegar por la Dark Net.[5] Aunque la bibliografía especializada ha reconocido la existencia de estos servicios de resolución de litigios, actualmente no hay ninguna publicación

4 Ortolani, P.: 'Self-enforcing online dispute resolution: lessons from Bitcoin' Oxf. J. Legal Stud., 2016, vol 36, pp. 595–629.

5 En el momento de escribir estas líneas, sólo conocemos dos trabajos científicos de criminólogos en los que examinan respectivamente los datos de los sistemas de resolución de disputas de dos foros de la Dark Web: el BHF.IO y el Dark0de, de Choi, K-S and Lee, CS,: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' *Journal of Contemporary Criminal Justice* 2023, vol. 39, num. 2, p. 201, y Dupont, B., y Lusthaus, J.: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' *Social Science Computer Review,* 2021, vol. 40 num 4, p. 892.

jurídica que examine los matices de los diferentes procesos de resolución de disputas empleados en la Dark Web, y mucho menos una discusión sobre cómo están surgiendo en forma de un ecosistema de derecho privado en la Dark Web. El presente estudio pretende contribuir a colmar la laguna existente en la investigación y así ampliar la limitada información existente sobre estos sistemas de justicia clandestinos que operan en la Dark Net. Con ello, este es el primer estudio jurídico que analiza el funcionamiento de estos mercados a un nivel macro, centrándose en los diversos procesos de resolución de conflictos empleados en la Dark Web, y argumenta que su crecimiento orgánico está contribuyendo a la aparición de un ecosistema de derecho privado en la Dark Web.

A tal fin, este estudio ofrece un análisis del alcance de las características y el funcionamiento de estos procesos de resolución de litigios basado principalmente en los escasos datos publicados, en el análisis cualitativo de los procesos de resolución de litigios que ofrecen los mercados de la Dark Web, y en los mensajes disponibles en estos mercados y foros donde los usuarios pueden presentar reclamaciones.[6] Al arrojar luz sobre la resolución de litigios en la Dark Web, este estudio pretende mejorar nuestro conocimiento sobre este campo y disipar las ideas erróneas sobre el gobierno anárquico en la Dark Web. Por consiguiente, en primer lugar, se analiza cómo los internautas acceden a la Dark Web. En segundo lugar, se examinan las principales herramientas de prevención de litigios integradas en los mercados de la Dark Web; a saber, los sistemas de reputación, la selección de los vendedores y la emisión de advertencias, especialmente de vendedores fraudulentos y sitios web espejo (*mirror sites*). En tercer lugar, el presente estudio analiza los principales procesos de resolución de litigios empleados en la Dark Web, que se dividen a grandes rasgos en procesos de negociación directa, mediación y adjudicación por parte del *escrow* y de los administradores del mercado. Por último, este estudio sostiene que estos sistemas emergentes de resolución de disputas tratan de aumentar la confianza en estos mercados y la proliferación de las transacciones ilícitas entre los usuarios, y por lo tanto están contribuyendo a la creación de un ecosistema de derecho privado para los ciberdelincuentes.

II. EL ACCESO A LA WEB OSCURA.

1. Los Diferentes Niveles de Internet.

Muchos pueden considerar que Internet y la World Wide Web (es decir, la web) son sinónimos, pero no lo son, ya que la web es sólo una sección de

6 El estudio y acceso a estos mercados en la Dark Web ha sido sometido al proceso de aprobación ética de la Universidad de Leicester.

Internet a través de la cual se puede acceder a la información.[7] Internet también puede utilizarse para otras actividades, como el envío de correos electrónicos, la transferencia de archivos o las videoconferencias.

Para explicar qué es la Dark Web, y en qué se diferencia de la Red Clara o la Clear Web, hay que distinguir los tres niveles de la Red: la Red Superficial (*Surface Web*), la Red Profunda (*Deep Web*) y la Red Oscura (*Dark Web*). La Red Superficial, también conocida como Red Pública (*Public Web*) o Red Clara (*Clear Web*), es la parte de la Red a la que se puede acceder a través de navegadores normales y motores de búsqueda.[8] Esto se debe a que los sitios web accesibles a través de estos navegadores están indexados, como muchas páginas web populares, mercados en línea, y plataformas de vídeos. Sin embargo, se calcula que sólo alrededor del 4% de Internet es accesible a través de la Red Superficial.[9]

A continuación, está la Red Profunda, también llamada la Red Invisible u Oculta (*Invisible* o *Hidden Web*), que representa la mayor parte de Internet. La Deep Web incluye los sitios que requieren que las partes se registren, y cuando el contenido que no ha sido indexado por los buscadores tales como Google, como la mayor parte de la información contenida en sitios de redes sociales, bancos, proveedores de correo electrónico y bases de datos legales como Lexis Nexis y Westlaw. Dentro de la Deep Web también hay redes privadas, conocidas como Intranets, que se construyen para las organizaciones de los usuarios, como universidades, administraciones públicas y grandes empresas.

Por último, la Dark Web, también conocida como Red Oscura, es una sección de la Deep Web que garantiza el anonimato de las partes y a la que sólo se puede acceder mediante un software especial porque su contenido se ha ocultado intencionadamente. En consecuencia, una red privada y segura que utiliza un protocolo criptográfico, a la que sólo puede acceder un grupo selecto de personas y no los navegadores de Internet normales, también sería un ejemplo de Dark Web. Sin embargo, la Dark Web es mucho más lenta que la Surface Web porque utiliza los canales traseros de Internet, y por la misma razón los sitios de la Dark Net no son tan ricos en imágenes como los mercados de la Surface Web. Al igual que en la Deep Web, el contenido de los sitios de la Dark Web no está indexado. No está claro, sin embargo, qué parte de la Deep Web está ocupada por contenidos de la Dark Web, y qué parte de la Dark Web se utiliza para actividades legales o ilegales.

7 Finklea, K.: 'Dark Web', Congressional Research Service, 7-5700, R44101 (10 marzo 2017) p. 2. Véase https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf. Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', Paper Series: No. 6 febrero 2015.

8 DeNicola, L.: 'What is the Dark Web?' *Experian - Cybersecurity* (12 mayo 2021). Véase https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

9 Ibid.

La Dark Web fue creada originalmente por el Laboratorio de Investigación Naval de Estados Unidos para proporcionar un mecanismo de comunicaciones privadas en línea al personal militar y a los espías.[10] El gobierno estadounidense decidió publicar el código para que a los espías les resultara más fácil ocultarse y permitir que otras personas, especialmente aquellas cuyos gobiernos restringen el uso de Internet, pudieran comunicarse de forma anónima. Por lo tanto la Red Oscura es un baluarte para la libertad de expresión en países como China, Siria, Afganistán y Korea del Norte. Así se creó la red TOR como navegador de código abierto y el Gobierno Federal de EE.UU. sigue siendo su principal financiador.[11] Por lo tanto, paradójicamente, el Gobierno de EE.UU. creó y financia la TOR, el cual permite acceder a la Dark Web donde la actividad ilícita prolifera entre usuarios anónimos que corren muy poco riesgo de ser detectados por las fuerzas de seguridad.

2. Entrar en la Dark Web.

La mayoría de los usuarios de la Dark Web acceden a ella a través de la red TOR.[12] TOR son las siglas de "The Onion Router", que hace referencia a las capas de encriptación que resemblan a una cebolla con el fin de proporcionar anonimato y privacidad a sus usuarios.[13] Para entrar en la Dark Web los usuarios necesitan primero instalar el navegador TOR, de acceso libre y uso legal. Las direcciones de los sitios de la Dark Net accesibles a través de la red TOR terminan en ".onion". En la red TOR, cada nodo sustituye la dirección IP del usuario por la suya propia y elimina secuencialmente una capa de cifrado. Por último, el servidor final, conocido como nodo de salida, descifra completamente su solicitud y la transmite al sitio deseado. Por consiguiente, las partes externas no pueden averiguar la dirección IP original ni establecer una conexión rastreable con sus actividades en línea. Esto se debe a que los sitios .onion no están en ningún registro central similar a como ICANN mantiene los nombres de dominio de la Web Clara. A pesar de ello, se han conocido casos en los que TOR ha revelado la dirección IP real del usuario a hackers especializados y servicios secretos como la Agencia de Seguridad Nacional (NSA) y el servicio secreto inglés (GCHQ).[14] Por eso, la mayoría de los usuarios de la Dark Net también emplean el cifrado de una Red Privada Virtual (VPN) para

10 Davies, G.: 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers' *Journal of Criminal Law,* 2020, vol. 84 num 5, 408.

11 Jardine, E.: 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' *Global Commission on Internet Governance Paper Series,* 2015, vol. 21, p. 6. Véase https://ssrn.com/abstract=2667711.

12 The Onion Router Project. Véase https://www.torproject.org/projects/torbrowser.html.en.

13 Finklea: 'Dark Web', cit. p. 2. Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', cit.

14 Electronic Frontier Foundation, 'GCHQ Leak: A Potential Technique to Deanonymise Users of the TOR Network' UK Top Secret Strap1 Comint, OPC-M/TECH.B/61 (13 June 2011). Véase https://www.eff.org/document/20141228-speigel-potential-technique-deanonymise-users-tor-network. Aminuddi, M., Zaaba, Z., Samsudin, A., Zaki, F. y Anuar, N.: 'The rise of website fingerprinting on Tor' *Journal of Network and Computer Applications,* 2023, p. 212.

ocultar la ubicación de su dirección IP y mantener la privacidad de sus actividades de navegación.

Aunque en la Dark Net hay foros y mercados que contienen actividades ilegales, también hay sitios legales, incluso de organismos públicos, como la CIA, que en 2019 lanzó su propio sitio para permitir comunicaciones seguras y anónimas con los usuarios de la Dark Web.[15] Del mismo modo, otros grandes medios de noticias, como el New York Times y el Washington Post, también tienen presencia en la Dark Web para permitir comunicaciones anónimas con informantes.[16] Incluso Facebook tiene ahora su propio sitio .onion, que en 2016 declaró tener más de un millón de usuarios.[17] Por lo tanto, la Dark Web no solo se utiliza para el comercio ilícito, sino que también la utilizan periodistas, informantes, disidentes y, en general, usuarios de Internet que no quieren ser rastreados. De hecho, Edward Snowden utilizó TOR para denunciar la vigilancia generalizada llevada a cabo por el Gobierno de Estados Unidos mediante la publicación de miles de documentos clasificados por la NSA.[18] La amplia repercusión y difusión de estas revelaciones tuvo un efecto dominó en el aumento de usuarios en la Dark Web.[19]

El presente artículo se centra en los mercados ilícitos donde los usuarios aprovechan su anonimato para comprar y vender una inquietante gama de bienes y servicios, como drogas, armas, falsificaciones, datos privados, pornografía infantil, *ransomware*, el alquiler de sicarios o la contratación de campañas de spam. Sin embargo, muchos mercados establecen restricciones sobre lo que se puede vender, y a menudo prohíben la venta de ciertos artículos que tienen más probabilidades de llamar la atención de las fuerzas de seguridad, como pornografía infantil, armas, fentanilo y asesinatos por encargo.[20]

Los mercados de la Dark Web también se conocen como criptomercados porque utilizan criptomonedas como Bitcoin y Monero que, especialmente la última, ofrecen un grado de anonimato en las transacciones. El anonimato se logra porque las transacciones se asocian con direcciones de billetera públicas, no con identidades personales directamente. Sin embargo, el anonimato no es completo. Las transacciones son públicas y permanentes en la cadena de bloques de Bitcoin, permitiendo que, con análisis suficiente y bajo ciertas circunstancias, se puedan

15 The Tor site of the CIA is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.

16 Véase https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/ y washingtonpost.securedrop.tor.onion. Todos los enlaces acabados en .onion son accesibles exclusivamente desde la Dark Web a través de TOR.

17 Véase facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion. Véase Hoffman, W.: 'Facebook's Dark Web .Onion Site Reaches 1 Million Monthly Tor Users' (22 abril 2016). Véase https://www.inverse.com/article/14672-facebook-s-dark-web-onion-site-reaches-1-million-monthly-tor-users.

18 Croy, A.: *The Dark Web: The Covert World of Cybercrime*, Greenhaven Publishing LLC, 2018, p. 30.

19 Doyle, E.: *The Dark Web*, Greenhaven Publishing LLC, 2019, p. 56.

20 Véase for example Nemesis, the Royal Market y ASAP Market.

rastrear a sus participantes. Por ejemplo, vinculando una dirección de billetera a una identidad real a través de transacciones en intercambios de criptomonedas que requieren verificación de identidad, se puede potencialmente descubrir quién ha hecho un pago.

Aprovechando los nodos TOR para ocultar sus direcciones IP, los usuarios pueden acceder a sitios no listados de forma anónima y pagar las transacciones también de forma anónima. Este anonimato fomenta la utilización de la Dark Web con fines ilícitos, ya que obstruye el rastreo de los usuarios por parte de las fuerzas de seguridad, garantizando la privacidad de los usuarios en estas redes públicas.[21] Sin embargo, la privacidad por sí sola no bastaría para atraer a una masa crítica de usuarios. Por ello, estas plataformas no sólo permiten a los usuarios ofrecer bienes y servicios y realizar transacciones, sino que también les proporcionan herramientas para evitar conflictos y sistemas de resolución de litigios.

III. HERRAMIENTAS PARA EVITAR DISPUTAS EN LA DARK WEB.

Los mercados en la Dark Net necesitan ofrecer garantías a los usuarios potenciales para que éstos puedan confiar en ellos y realizar transacciones. Estas garantías se proporcionan incorporando en su diseño herramientas que reducen el riesgo de que surjan disputas en primer lugar. En consecuencia, los mercados de la Dark Web incorporan características de seguridad, advierten a los usuarios sobre la suplantación de identidad (*phishing*), los sitios espejo (*mirror sites*), vetan a sus vendedores, y proporcionan a los usuarios información sobre las transacciones anteriores de los vendedores, como el número de transacciones completadas y las opiniones de otros compradores anteriores.

1. Elementos de seguridad.

Las características de seguridad de los mercados buscan garantizar el anonimato de los usuarios y evitar interferencias de *hackers* y robots (*bots*). Además del uso del navegador TOR y la VPN, para acceder a la mayoría de los mercados se requiere que los usuarios se registren primero eligiendo un nombre de usuario y una contraseña. El inicio de sesión normalmente tiene un CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), en el que se puede pedir al usuario que identifique los cuadrados que no pertenecen a una fotografía o que vuelva a escribir las letras o números que aparecen en una imagen.

Para completar una transacción en la que se van a entregar bienes en una dirección física, se pide al comprador que encripte su nombre y dirección utilizando la clave pública PGP del vendedor. Aunque algunos usuarios pueden utilizar una

21 Davies, 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers', cit., p. 408.

identidad falsa, la mayoría utilizan sus datos personales reales para evitar sospechas por parte del servicio de correos o del cartero.[22] Además, algunos mercados, como ASAP Market, recomiendan a los usuarios que empleen la autenticación de dos factores (2FA).

Lo más importante es que el pago de la transacción se realiza de forma anónima utilizando criptomoneda que se deposita en el *escrow*. De hecho, la mera existencia del *escrow* produce un nivel de confianza entre las partes implicadas, ya que ni el comprador ni el vendedor tienen control sobre los fondos hasta que se cumplan las condiciones contractuales, lo que reduce el riesgo de fraude.

Para reducir el riesgo de que las fuerzas de seguridad relacionen los bitcoins con la identidad de los usuarios, lo que de por sí requiere una investigación, los usuarios, y especialmente los grandes vendedores, pueden emplear un *tumbler* de criptodivisas (también conocido como servicio de mezcla), que desidentifica el origen de la criptodivisa mezclándola con otras antes de devolverla en diferentes lotes. Dado que estos servicios permiten el blanqueo de dinero, varios proveedores han sido el objetivo de las fuerzas de seguridad.[23]

2. Expulsión, veto y advertencias.

Los administradores de los mercados en la Dark Net tienen como prioridad la expulsión de los vendedores poco fiables y garantizar el anonimato de sus usuarios. Para ello, los pagos deben realizarse siempre mediante criptomoneda. Más aun, solicitar otro tipo de pago, como una transferencia de Western Union o una transferencia bancaria, conllevará una prohibición permanente en dicho mercado.[24] En una línea similar, los vendedores que tengan un alto índice de disputas serán vetados. Por ejemplo, ASAP Market prohíbe la entrada a los vendedores con más de un 30% de disputas entre sus ventas.[25]

El anonimato puede plantear riesgos a los usuarios, y no sólo frente a vendedores fraudulentos, sino también frente a las fuerzas de seguridad, ya que los usuarios no pueden estar seguros de que la persona que ofrece un producto o servicio no sea un agente encubierto o un informante de la policía.[26] Para reducir estos riesgos, se exige a los vendedores habituales que paguen una cuota de entrada

22 Afilipoaie, A., y Shortis, P.: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' *Global Drug Policy Observatory, Situation Analysis*, 2015, p. 4.

23 US Department of Justice - Office of Public Affairs, 'Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"' (28 abril 2021). Véase https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

24 Véase ASAP Market Rules. Disponible en el siguiente enlace de la Dark Web http://asap4u7rq4tyakf5gdahmj2c77blwc4noxnsppp5lzlhk7x34x2e22yd.onion.

25 Ibid.

26 Campana, P., y Varese, F.: 'Cooperation in criminal organizations: Kinship and violence as credible commitments' *Rationality and Society,* 2013, vol. 25, num 3, p. 265.

antes de permitirles operar como vendedores en el mercado. La cuota no suele ser reembolsable y pretende disuadir a los vendedores fraudulentos, que serán expulsados del mercado si no respetan las normas estafando a los compradores, o si no acatan una decisión tomada en el proceso de resolución de conflictos. El valor de la tasa varía en función del mercado, pero cuanto mayor sea éste, mayor será la tasa. Por ejemplo, Nemesis exige a los vendedores una cuota de entrada de 500 USD, mientras que Royal Market cobra 1.000 USD. Otros mercados sólo admiten a vendedores con experiencia y reputación que hayan participado en otros mercados. Por ejemplo, para ser admitido en CannaHome Market un vendedor necesita tener al menos 500 ventas en otros mercados y valoraciones de 4 estrellas o menos de un 1% de opiniones negativas de clientes anteriores. Por lo tanto, las fianzas de los vendedores contribuyen a que los mercados obtengan beneficios, al tiempo que disuaden a posibles estafadores de aprovecharse de usuarios inexpertos.[27]

Las estafas y los enlaces falsos a mercados que pretenden estafar a los compradores mediante el uso de espejos (*mirror sites*) son un riesgo habitual para los usuarios de la Dark Web. Un espejo es esencialmente una copia de un sitio (*website*) que permite a los usuarios acceder a la misma información que en el sitio original, y donde cualquier cambio en el sitio espejo se producirá automáticamente en el sitio original. Sin embargo, también existen espejos maliciosos utilizados por individuos que suplantan su identidad (*phishers*) que parecen el sitio original, pero a cuyos usuarios se les copian los datos de acceso y se les cambia la dirección de pago por la del estafador. Habitualmente, el usuario no se da cuenta de la estafa hasta que presenta una reclamación en el mercado y se da cuenta de que el vendedor o el mercado no han recibido el pago. Para advertir de estos riesgos, los administradores de los mercados de la Dark Web suelen publicar mensajes en forma de banners o anuncios en el foro del mercado advirtiendo sobre los estafadores y los enlaces falsos al mercado.

3. Sistemas de reputación.

Al igual que la reputación de los vendedores y los comentarios de los compradores son cruciales en el comercio electrónico de la Surface Web, en la Dark Web los usuarios utilizan seudónimos para comunicarse y pueden dejar comentarios después de cada transacción con una calificación numérica, así como un comentario explicando su calificación.[28] Esta información se aporta cuando termina la transacción, es decir, cuando el comprador ha recibido la mercancía y el vendedor ha recibido los fondos del proveedor de custodia (*escrow*). Una

27 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net', cit., p. 3.

28 Cybersixgill, 'Trust on the Deep and Dark Web' (22 marzo 2022). Véase https://cybersixgill.com/news/articles/trust-on-the-deep-and-dark-web.

vez finalizado el pedido, las partes no pueden impugnar la transacción. Algunos sistemas de evaluación tienen en cuenta otros factores además de las opiniones de los compradores y permiten a los vendedores evaluar a los compradores, con lo que se pretende identificar a los compradores que hacen reclamaciones falsas con el fin de obtener un reembolso del pago.[29] No obstante, las opiniones positivas de los compradores son especialmente importantes para que los vendedores atraigan el regreso de clientes, así como de nuevos compradores.

Prestar atención a la reputación de los vendedores es vital para reducir el riesgo de litigios e identificar a los vendedores reputados, mitigando así los riesgos de fraude.[30] Los sistemas de reputación desempeñan un papel fundamental a la hora de fomentar la comunicación eficaz, la cooperación y la confianza en las transacciones, disminuyendo así la probabilidad de malentendidos y conflictos.[31] Cuando surge una disputa, las partes con buena reputación son más propensas a entablar discusiones constructivas y a trabajar para encontrar soluciones amistosas. Además, las revisiones ayudan a incentivar a los vendedores para que se adhieran a las decisiones tomadas en el proceso de resolución de disputas. De hecho, los vendedores suelen esforzarse por proteger su reputación en estos mercados, ya que perder la confianza o ser expulsados reducen su capacidad para seguir comerciando.

En el ámbito de la ciberdelincuencia, los administradores y moderadores de los mercados de la Dark Web asumen una función policial al impedir activamente que los estafadores (a menudo denominados *rippers*) participen en las actividades del mercado ilícito. Esto sirve tanto para disuadir a los defraudadores potenciales como para aumentar la confianza y la fiabilidad del mercado. En consecuencia, la forma de acción disciplinaria más frecuente en estos mercados es el ostracismo mediante la aplicación de medidas de suspensión y expulsión.[32]

Según un estudio empírico de tres mercados de la Dark Web (Wallstreet Market, Hansa Market y AlphaBay), las valoraciones positivas constituían más del 90% de todas las valoraciones de cada uno de los tres mercados.[33] También se descubrió que el mayor porcentaje de valoraciones neutras y positivas se daba en el más pequeño de los tres mercados, lo que puede deberse a que resultaba

29 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net', cit., p. 5.

30 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', 2023 p. 14. Véase https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/03/10151223/Business-on-the-dark-web-deals-and-regulations.pdf?reseller=gl_regular-sm_acq_ona_oth__onl_b2b_securelist_lnk_sm-team.

31 Holt, T.: 'Exploring the social organisation and structure of stolen data markets' *Global Crime* vol. 2013, num. 14(2-3), pp. 155–174 y Yip, M. , Webber, C., Shadbolt, N.: 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing' *Policing and Society*, 2013, vol. 23, num. 4, pp. 516–539.

32 Holt, T. y Lampke, E., 'Exploring stolen data markets online: Products and market forces' *Criminal Justice Studies*, 2010, vol. 23, num. 1, pp. 33–50.

33 Lummen, DLM: 'Is Telegram the new Dark Net? A comparison of traditional and emerging digital criminal marketplaces' (MSc thesis, University of Twente 2023), p. 49.

menos atractivo para los estafadores que los mercados más grandes.[34] Por tanto, los vendedores de la Dark Web dependen de la reputación para hacer negocios, y una mala reputación puede ser devastadora con respecto a las futuras transacciones y su posición competitiva con otros vendedores. Además, cuando surgen disputas, los árbitros tienen en cuenta las reseñas del vendedor y el historial del comprador, por lo que aquellos con mayores reseñas positivas e historial de transacciones tienen más probabilidades de que el proceso de solución de disputas se incline a su favor. Algunos mercados oscuros, como Archetyp, también informan a los compradores y a los árbitros el número de disputas o reclamaciones abiertas que tiene el vendedor. Este sesgo inherente en el proceso de resolución de disputas podría llevar a los vendedores experimentados a ser selectivos y aprovecharse exclusivamente de los compradores sin experiencia.

IV. PROCESOS DE RESOLUCIÓN DE DISPUTAS EN LA DARK WEB.

Cuando un comprador realiza un pedido, lo hace a través de un mensaje privado enviado al vendedor donde indica los artículos que desea comprar y la dirección para la entrega, mientras que el vendedor proporciona el enlace para realizar el cripto-pago en su monedero electrónico, o en el del servicio de custodia (*escrow*). Dado que la dirección del comprador (ya sea digital o física) es un dato personal sensible que los compradores no quieren que esté disponible en la Dark Web, se les recomienda que la cifren utilizando la clave PGP pública de los vendedores, para que éstos puedan descifrar la dirección del comprador utilizando su clave privada. Ello evita que terceros interceptores puedan leer el mensaje. Sin embargo, los compradores inexpertos que no sepan utilizar PGP pueden realizar pequeños pedidos con éxito sin cifrar los datos personales, pero la mayoría de los vendedores insisten en proporcionar el cifrado y pueden ignorar la información que no haya sido cifrada.[35] Una vez recibido el pago en la dirección del monedero electrónico facilitada por el vendedor, éste enviará los artículos comprados y borrará el texto cifrado.

Si las partes tienen problemas con su transacción, pueden discutir una solución utilizando la sala de mensajes privados abierta para la transacción. El vendedor puede presentar una reclamación si no ha recibido el pago. Sin embargo, esto no es muy habitual, ya que los vendedores normalmente cancelan una transacción que no ha sido pagada en un plazo determinado, que puede ser de unas horas o hasta unos días desde que el comprador realizó el pedido. Los compradores, no obstante, son los reclamantes paradigmáticos cuando no han recibido la mercancía en el plazo previsto, o cuando los artículos adquiridos funcionan mal, como los

34 Ibid.

35 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' cit., p. 2.

litigios relativos a programas maliciosos, como los de ransomware, ineficaces, o cuando la calidad de los bienes no se ajusta a su descripción, como los litigios relativos a la baja calidad de las drogas o medicamentos. Aunque el valor de la mayoría de los litigios oscila entre unos cientos y unos miles de dólares, se han registrado casos de mayor cuantía, como uno de dos millones de dólares por servicios de piratería informática.[36] De hecho, hay pruebas de que algunos consumidores compran drogas a granel en la Dark Web para venderlas después en cantidades más pequeñas,[37] por lo que estos mercados pueden funcionar tanto como mayoristas como minoristas, permitiendo transacciones de alto y bajo valor.

Cuando no existen mecanismos para resolver disputas en la Dark Web, hay un mayor riesgo de que las disputas deriven en violencia u otras actividades ilegales, como el chantaje o la extorsión, que pueden ser utilizadas por los vendedores para resolver las disputas a su favor. Así pues, los compradores estarán especialmente expuestos a estos riesgos cuando hayan facilitado a los vendedores su domicilio para la entrega de los artículos adquiridos.

Cuando surge un litigio, las partes intentan negociar una solución. Si no se puede llegar a un acuerdo, los usuarios recurrirán al servicio de custodia o al administrador del mercado, que investigará la reclamación y tomará una decisión definitiva sobre el resultado de la disputa. Cuanto mayor sea el mercado, más probable es que tenga un equipo de atención al cliente dedicado a resolver disputas. Este es el caso de Tor2door, que ofrece un servicio de resolución de disputas 24 horas al día. Ambas partes aceptan el proceso cuando realizan una transacción en el mercado, y como ambas partes quieren mantener el pago de la transacción, están incentivadas a participar en el proceso de resolución de disputas. Los principales procesos de resolución de disputas en la Dark Web son la negociación, que a veces se apoya en un proceso que trata de identificar las cuestiones en disputa, y la mediación y adjudicación proporcionadas por el servicio de custodia o el moderador del mercado. Estos procesos se examinan a continuación.

1. Negociación entre las partes.

Los mercados de la Dark Web recomiendan que los reclamantes se comuniquen primero directamente con la otra parte para aclarar cualquier malentendido y explorar una resolución rápida. Un estudio empírico a pequeña escala de 201 casos en el foro en ruso BHF.IO descubrió que los acuerdos tardaban una media

36 Vijayan, J.: 'The Dark Web has its own people's court' (7 diciembre 2021) Dark Reading. Véase https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts.

37 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' cit., p. 4.

de 3,05 días desde la presentación de la disputa, mientras que las adjudicaciones tardaban 6,77 días. [38]

Las comunicaciones directas se producen normalmente a través del sistema de mensajería privada disponible en el mercado y busca lograr una resolución confidencial y rápida. La sala privada puede ser la misma que se abrió para completar la transacción, o puede ser una nueva sala de chat abierta por el reclamante. Además de los mensajes privados, algunos mercados que han cerrado, como AlphaBay, ofrecían a las partes un servicio automatizado de resolución de disputas llamado *Automatic Dispute Resolver.*[39] Básicamente, se trata de un sistema de resolución en el que el comprador y el vendedor pueden ampliar el tiempo de custodia, acordar reembolsos totales o parciales u opciones de sustitución. Este proceso de negociación imita los pasos que, de otro modo, habría dado un administrador del mercado durante un proceso de resolución de disputas. En los casos en que las partes no puedan llegar a un acuerdo, permite a las partes indicar sus opciones de resolución preferidas, lo que facilita el papel del administrador del mercado en la resolución de litigios. Cada parte puede aceptar o negar las resoluciones propuestas por la otra parte.

AlphaBay también ha creado un sistema llamado *Streamlined Dispute Process* para gestionar las reclamaciones a través de conversaciones por mensaje privado, que se eliminan de los pedidos una vez resueltas.[40] A través de este sistema las reclamaciones van a una sección diferente de la web. Si las partes no alcanzan un acuerdo, la disputa pasa al modo manual donde los administradores pueden ver las interacciones no cifradas, así como las propuestas de acuerdo, y resolver la disputa pendiente.

Cuando las partes no pueden llegar a un acuerdo, el reclamante suele tener la opción de hacer clic en "Disputa" en la página del pedido para remitir la reclamación al foro de resolución de disputas previsto por el mercado.[41] Algunos mercados tienen un foro público en el que se publican las disputas y se invita a la comunidad a compartir sus opiniones sobre la disputa. Las opiniones de los usuarios pueden persuadir a las partes para llegar a un acuerdo amistoso, que puede implicar que el demandado ceda en parte o en la totalidad de la reclamación. Además, los usuarios del mercado, especialmente los más novicios, pueden utilizar el foro de los mercados para pedir consejo sobre la conveniencia de iniciar disputas contra

38 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 208.

39 Onion Index, 'AlphaBay' (*GitHub,* 1 diciembre 2022) https://github.com/OnionIndex/AlphaBay; y 'AlphaBay Market | Home' (*AlphaBay*) https://alphabay-url.com/ .

40 Ibid.

41 DoingFedTime, 'Dispute Resolution Buyers vs Vendors – Deep Dot Dark Net' (27 noviembre 2022). https://www.youtube.com/watch?v=qwZvflkl-9c&t=12s.

otros vendedores. Así, al facilitar las interacciones entre los usuarios del mercado, permitiéndoles expresar sus opiniones sobre el fundamento de la reclamación, el foro público anima a las partes a llegar a un acuerdo mediante esta técnica colaborativa de resolución de problemas.

La promoción de la negociación como fase inicial del servicio de resolución de litigios reconoce que muchos conflictos pueden resolverse sin la intervención de terceros. Además, la privacidad de estas negociaciones evita la escalada innecesaria de las reclamaciones y reduce el riesgo de hacer acusaciones infundadas que difamen injustificadamente a la otra parte en el foro del mercado.

2. El sistema de custodia (*escrow*): mediación y adjudicación.

Los servicios de custodia (*escrow*) son el ingrediente clave de la Dark Net para superar el riesgo de transacciones fraudulentas. El servicio de custodia lo proporciona el mercado, y suele ser la principal fuente de ingresos del mercado, ya que cobra una comisión por transacción, que puede llegar al 10% del valor de la venta, aunque lo más habitual son comisiones más bajas, entre el 5% y el 2%.[42]

Según un estudio, el 85% de los mercados de la Dark Web utilizan agentes de custodia para cada transacción,[43] que retienen los pagos del comprador y los liberan al vendedor cuando éste confirma que el producto se ha entregado, o el servicio se ha prestado adecuadamente. Los fondos también pueden ser liberados sin la confirmación del comprador después de un período previamente acordado o después del tiempo establecido por el mercado (usualmente referido como orden 'Auto Finalizada'). Por ejemplo, Tor2door Market establece catorce días para los productos físicos y dos días para los productos digitales. Las partes pueden ampliar el plazo de custodia. En el caso de Tor2door, los compradores pueden solicitar dos veces una prórroga de cinco días a partir del noveno día desde que el vendedor marca el pedido como enviado. Es importante destacar que la disputa sólo puede plantearse antes de que se finalice el pedido (y se realice automáticamente el pago al vendedor).

Los vendedores más reputados del mercado pueden vender sus productos y servicios sin depósito de garantía, operando como vendedores cuyos pagos se realizan directamente en sus monederos electrónicos. A estos vendedores se identifican como transacciones que "finalizan pronto" (*Finalize Early* o *FE*), Los requisitos para entrar en esta categoría son bastante exigentes. Por ejemplo, ASAP Market exige a los vendedores más de 10.000 ventas y más de un 99%

42 White, G., y Archampong, P.: The Dark Web, Episode 7, Cybercrime Inc, Podcast, (8 febrero 2018).

43 HP Wolf Security et al, 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape y How to Fight Back – An HP Wolf Security Report' (julio 2022). https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf p. 15.

de opiniones positivas. Aunque estos vendedores no pueden ofrecer las mismas garantías que un tercero, dada su posición establecida en el mercado, es más probable que sigan las instrucciones del administrador del mercado.

Cuando un comprador no está satisfecho con la transacción, se presenta una reclamación ante el agente de custodia (normalmente el administrador del mercado, pero también puede ser un tercero), que congelará el importe de la custodia, examinará las pruebas y determinará quién se quedará con los fondos de la transacción. Sin embargo, antes de que el agente de custodia resuelva el litigio, suele haber un debate moderado por el tercero, similar a un mediador, que trata de explorar un acuerdo.

Cuando es el agente de custodia (*escrow*) quien actúa como tercero, el nombramiento no lo hace el administrador del mercado,[44] en su lugar, las partes se ponen en contacto directamente con el proveedor de custodia y plantean la disputa. Por el contrario, la mayoría de los mercados, como ASAP Market, proporcionan y controlan el sistema de custodia. No obstante, cuando la reclamación se hace directamente al fondo de custodia, la resolución de la disputa se realiza de manera privada.

3. El administrador del mercado: mediación, crowd ODR y adjudicación.

Cuando un sistema de custodia está controlado por el mercado, o cuando el dinero ya se ha transferido al vendedor, los reclamantes pueden publicar su queja en una sección específica del mercado, donde los administradores (o sus moderadores designados por éstos) examinan las pruebas presentadas por las partes y resuelven la disputa. A diferencia de una custodia externa, los administradores del mercado tienen competencias punitivas y reparadoras exclusivas, como la de prohibir al demandado la entrada en el mercado o pedirle que indemnice al demandante.[45]

Si el pago se hubiera depositado en el sistema de custodia facilitado por el mercado, entonces el dinero podrá transferirse a la parte ganadora. Pero, como se ha señalado anteriormente, incluso cuando el dinero no haya sido depositado en el *escrow*, y en su lugar ya haya estado en posesión del vendedor, el éxito de la futura participación de los vendedores en el mercado dependerá del cumplimiento del resultado, ya que los compradores no adquirirán bienes o servicios de vendedores que no cumplan estas resoluciones.[46] Además, el incumplimiento de la resolución puede dar lugar a la expulsión de la parte perdedora del mercado.

44 Kapersky: 'Business on the dark web: Deals and regulatory mechanisms', cit., p. 7; Mirea, M., Wang, V., y Jung, J.: 'The not so dark side of the Dark Net: a qualitative study' SJ, 2019, vol. 32, p. 105.

45 Dupont y Lusthaus: Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' cit., p. 906.

46 Ibid.

Del mismo modo, en caso de que se constate un comportamiento fraudulento, el administrador expulsará a la parte responsable. Dado que la mayoría de los demandados son vendedores que quieren seguir operando en el mercado, normalmente acatarán el resultado y reembolsarán al comprador cuando así se lo indique el administrador.[47]

El proceso de resolución de disputas comienza cuando los compradores o vendedores denuncian su disputa en la sección de resolución de disputas del mercado. Algunos mercados tienen dos secciones de resolución de disputas, una para disputas contractuales y otra para denunciar estafas y ataques virtuales.[48] Por ejemplo, Exploit, XSS, BreachForums y Verified tienen dos salas distintas para presentar reclamaciones, una de arbitraje, y otra para reclamaciones fraudulentas, que Exploit denomina "Blacklist" y XSS "Ripper List". Dentro de las salas de arbitraje, el proceso de resolución consiste en una adjudicación que no está naturalmente sujeta a la normativa de arbitraje, ya que no necesita de los tribunales para la ejecución de las decisiones. Cuando la disputa se ha realizado en un foro público, la decisión se emitirá después de que otros usuarios del mercado hayan tenido la oportunidad de compartir sus opiniones. Cuando un demandado acepta la reclamación, lo que es más probable que ocurra en transacciones de menor valor, el resultado suele ser la devolución parcial o total del criptopago realizado en la venta disputada. Más comúnmente, cuando el demandado impugna la reclamación, el administrador adjudica la reclamación a la vista de las pruebas aportadas por las partes, y cuando no hay pruebas suficientes para sostener la reclamación, entonces ésta será desestimada.

Los usuarios que deseen denunciar una estafa deben crear un nuevo hilo de conversación, identificar al usuario que supuestamente les ha estafado y proporcionar todos los detalles posibles sobre el incidente. Algunos mercados, como BreachForums, ofrecen una plantilla para denunciar las estafas.[49] A continuación, un moderador revisa la denuncia, pide más información si es necesario y etiqueta al acusado, dándole un plazo para responder, que suele ser de 24 horas, pero que puede variar en función de la gravedad del caso y del mercado. Por ejemplo, el Chinese Market establece un límite de tres días por el que, si una de las partes no contesta antes de que expire el plazo, la resolución se decidirá a favor de la otra parte. Del mismo modo, el Royal Market establece que, si una de las partes no responde en un plazo de 72 horas, el caso se decidirá probablemente a favor de la parte activa. Otros mercados tienen plazos más largos, como Nemesis, que

47 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 204.

48 Wixey, M.: 'The scammers who scam scammers on cybercrime forums: Part 1' (*Sophos*, 7 diciembre 2022) https://news.sophos.com/en-us/2022/12/07/the-scammers-who-scam-scammers-on-cybercrime-forums-part-1/.

49 Ibid.

tiene un plazo de siete días. A diferencia de lo que ocurre en las salas de arbitraje, donde las discusiones son en gran medida civiles y las partes pueden incluso llegar a un acuerdo amistoso, cuando se presenta una denuncia por estafa es más habitual que las partes caigan en insultos personales. De hecho, el lenguaje soez no es inusual en la Dark Web, incluso entre los comentarios de los administradores.

En la mayoría de los casos, el proceso de adjudicación sigue un formato informal. En el mercado Dark0de, que funcionó de 2007 a 2015, y que fue reabierto semanas después tras ser incautado por el FBI,[50] no se designó a un adjudicador como tal, dejando que los administradores decidieran su propio papel, que puede ser puramente facilitador, o adoptar el papel de adjudicador.[51] Del mismo modo, en el Mercado Hydra, los miembros de la comunidad del mercado pueden aportar testimonios, aunque, a diferencia del Dark0de, en este mercado el administrador siempre dicta una resolución final cuando las partes no pueden llegar a un acuerdo.[52] Por el contrario, algunos mercados ofrecen procesos privados. Aquí es donde entra en juego el Procedimiento Privado de Reclamación (PCP) por el que, en lugar de hacer público el asunto iniciando una reclamación en el sub-foro, el reclamante puede dirigirse en privado al administrador para solicitar la resolución de la disputa a puerta cerrada.[53]

Mientras que las comunicaciones de las partes suelen cifrarse mediante PGP, una vez que se presenta una disputa, las partes no deben cifrar los mensajes para que el administrador pueda leerlos. El formulario de reclamación suele estar estandarizado, y requiere que los reclamantes incluyan información sobre los nombres de usuarios de las partes, su información de contacto (por ejemplo, dirección de correo electrónico o perfil de Telegram), la cuantía de la reclamación, una breve descripción de la disputa, la petición que se solicita en la reclamación y las pruebas que apoyan la reclamación (por ejemplo, registros de chat, capturas de pantalla, registros de transacciones de criptomoneda, etc).[54] Aunque la reclamación puede publicarse en el sub-foro, las pruebas no suelen publicarse en dicho sub-foro, sino que se envían en privado al administrador. Esto se debe

50 Europol 'Cybercriminal Darkode Forum Taken Down Through Global Action' (15 julio 2015). Véase https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action y Stevenson, A.: 'It only took 2 weeks for the world's most dangerous hacking forum to get back online after the FBI shut it down' Insider (28 July 2015). Véase https://www.businessinsider.com/darkode-admin-returns-with-new-and-improved-hacking-site-2015-7?r=US&IR=T.

51 Dupont y Lusthaus: Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 905.

52 Social Links, 'Top-10 OSINT and Cyber Security Stories of 2022' (*Social Links*, 28 diciembre 2022) https://blog.sociallinks.io/top-10-osint-and-cyber-security-stories-of-2022/.

53 Dupont y Lusthaus: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 899.

54 Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading*, 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts; y Choi y Lee, : 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p.216; y Vanian: 'Online criminals have created their pseudo court system on the dark web' cit.

a que las partes serían reacias a proporcionar información que pudiera revelar su identidad o comprometer su seguridad, como proporcionar pruebas de que los artículos comprados han sido entregados en la dirección designada. Por ello, este tipo de información suele enviarse directamente a través de mensajes privados al administrador. Como no es aconsejable descargar nada en la Dark Web, para subir imágenes los usuarios emplean un software especializado, como filehole.org, que permite acceder a documentos y archivos a través de un enlace.

Una vez presentada la reclamación en el sub-foro, normalmente en cuestión de horas, el tercero neutral se pondrá en contacto con el demandado y le pedirá pruebas sobre la transacción en litigio.[55] En algunos casos, el tercero neutral abrirá un sub-foro independiente en el que otros usuarios del mercado podrán aportar sus opiniones sobre el caso.[56] Este proceso se asemeja al sistema de resolución colectivo (también conocido como *crowd online dispute resolution*), en el que un grupo de usuarios actúan como jurados resolviendo las disputas.[57] Sin embargo, a diferencia de los jurados de los tribunales o de los procesos de *crowd-ODR*, las opiniones de los usuarios no son vinculantes, ya que sólo los administradores (o sus terceros neutrales designados) tienen plena autoridad para adjudicar el resultado de la disputa.[58] En este modelo, todos los usuarios del mercado pueden publicar sus opiniones y comentarios en el sub-foro. Aunque sus opiniones no influyan necesariamente en el resultado del litigio, su capacidad para ver y comentar el fondo de la demanda va más allá del principio de justicia abierta, ya que los usuarios no son meros observadores, sino terceros intervinientes (también conocidos como *amicus curia*e en el contexto de los litigios judiciales),[59] cuyas opiniones buscan influir en última instancia en la decisión de las partes de llegar a un acuerdo o en la decisión final del administrador.

Aunque los administradores gozan de plena discrecionalidad para adoptar sus decisiones, éstas se basan en las pruebas aportadas por las partes y se ajustan a las normas del mercado y a los términos y condiciones de la transacción. El criterio de prueba utilizado se asemeja al empleado en el derecho privado inglés

55 Vanian, ibid; CyberSec_Sai, 'Did You Know Darkweb Has Its Own Courts and Justice System?' (*Medium*, 8 marzo 2023) https://medium.com/geekculture/did-you-know-darkweb-has-its-own-courts-and-justice-system-7ecfa25c46c8; Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 216.

56 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p. 13.

57 Raymond, A. y Stemler, A.: 'Trusting Strangers: Dispute Resolution in the Crowd' *Cardozo Journal of Conflict Resolution,* 2014, vol. 16, p. 357.

58 Bisson, D., 'How a Cyber Criminal Justice System Resolves Disputes' (*Security Intelligence,* 26 enero 2022) https://securityintelligence.com/news/cyber-criminal-justice-system-resolves-disputes/; Analyst1, 'Dark Web – Justice League' (*Analyst1,* 2021) https://analyst1.com/dark-web-justice-league/; Mujezinovic, D.: 'How to Police Hackers: Inside the Dark Web's Justice System' (*MakeUseOf,* 31 diciembre 2021) https://www.makeuseof.com/inside-dark-webs-justice-system/; Bracken, B.: 'When Scammers Get Scammed, They Take It to Cybercrime Court' (*threat post,* 7 diciembre 2021) https://threatpost.com/scammers-cybercrime-court/176834/.

59 Krislov, S., 'The Amicus Curiae Brief: From Friendship to Advocacy' *Yale Law Journal,* 1963, vol. 72, p. 694.

del balance de probabilidades. La carga de la prueba recae en el demandante, que debe convencer al administrador del fundamento de su reclamación, pero si el demandado no responde, puede ser suspendido o expulsado permanentemente del mercado.

Tanto si las partes llegan a un acuerdo como si es un tercero el que resuelve la reclamación, la decisión final suele publicarse en el sub-foro.[60] Sin embargo, se han dado casos en los que el administrador ha accedido a la petición del demandado de borrar la reclamación para proteger la reputación del vendedor frente a futuros compradores.[61] Por lo tanto, la eliminación de la reclamación queda a discreción del administrador, pero se espera que los demandados acaten el resultado antes de que se elimine el mensaje del foro. La petición de borrar la reclamación ilustra lo importante que es la reputación para los vendedores.

Si se estima la demanda, el procedimiento suele terminar con la obligación de indemnizar al demandante por una parte o por el coste total de la transacción. Si el demandado es declarado responsable pero no devuelve el dinero en el plazo fijado por el administrador, suele ser expulsado del mercado y añadido a la lista de miembros poco fiables de la comunidad. En esencia, se trata de una "lista negra" (a veces denominada "lista de defraudadores" o simplemente "doxing") que indica no sólo el nombre de usuario, sino que también puede incluir el nombre del mercado, el motivo de la prohibición y otros datos identificativos, como las criptomonedas o monederos electrónicos utilizados, correos electrónicos y apodos empleados en otros mercados de la Dark Net.[62] Otras consecuencias menos comunes incluyen el "swatting", que consiste en hacer una llamada a la policía para que acuda al lugar donde se encuentra el objetivo.[63]

Con todo, la consecuencia más común para un demandado que no acata la decisión del adjudicador es su expulsión del mercado.[64] Los demandantes también pueden ser vetados por presentar demandas frívolas. Además, si una o ambas partes no han seguido las normas del mercado, el administrador puede enviarles advertencias, suspenderles durante un periodo de tiempo o prohibirles el acceso de forma permanente. Una suspensión temporal puede consistir en que el administrador bloquee la cuenta del demandado hasta que se emita el

60 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p.13; Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 206.

61 Ibid, p. 213.

62 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p.13.

63 Lusthaus, J.: *Industry of anonymity: Inside the business of cybercrime*, Harvard University Press, 2018.

64 Bisson: 'How a Cyber Criminal Justice System Resolves Disputes' cit. Mujezinovic: 'How to Police Hackers: Inside the Dark Web's Justice System' cit.; Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading,* 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts; Wixey: 'The scammers who scam scammers on cybercrime forums: Part 1' cit.

reembolso.[65] Una vez publicada la decisión, si las normas del foro lo permiten, las partes pueden apelar la decisión ante otro tercero neutral o ante el administrador que presida el caso. Sin embargo, lo habitual es que la apelación solo pueda tener lugar después de que se haya ejecutado la decisión inicial.

V. EL SURGIMIENTO DE UN ECOSISTEMA DE DERECHO PRIVADO EN LA DARK WEB.

El presente estudio examina cómo la mayoría de los usuarios que participan en el comercio ilícito de la Dark Web tienen acceso a un proceso de resolución de litigios, que a menudo se apoya en un sistema de custodia y en herramientas para evitar litigios, tales como la fianza exigida a los vendedores, advertir a los usuarios de los riesgos fraudulentos e incorporar un sistema de reputación para los vendedores. Cuando las partes no pueden llegar a un acuerdo, normalmente pueden presentar una reclamación poniéndose en contacto con el agente de custodia o con el administrador del mercado (u otro árbitro designado por el administrador) para resolver el litigio en equidad de forma expeditiva basándose en las normas del mercado de la Dark Web donde haya tenido lugar la transacción y en las condiciones contractuales de la transacción. De este modo, en la Dark Net está surgiendo un ecosistema de derecho privado para resolver las disputas que surgen en los mercados ilícitos, similar a la forma en que la *lex mercatoria* y el arbitraje surgieron en Europa durante la Edad Media como una vía más adecuada para resolver las disputas entre los comerciantes internacionales que llegaban por la Ruta de la Seda y por otros itinerarios.

En esta última sección se examina, por un lado, la aparición de un ecosistema de derecho privado que busca aumentar la confianza en el usuario del mercado para fomentar el comercio (ilícito) y, por otro, se explican los rasgos definitorios de los procesos de resolución de disputas ofrecidos en la Dark Web, que se caracterizan por su eficacia (ya que son fácilmente accesibles, gratuitos y muy rápidos), informalidad (las partes se auto-representan), anonimato (ocultan los datos personales de los usuarios y de los terceros neutrales que dirimen las disputas) y porque se basan en mecanismos de auto-ejecución dada su naturaleza extralegal. Además, se argumenta que, aunque estos procesos no pueden garantizar el cumplimiento de las garantías procesales bajo supervisión judicial, los administradores de los mercados tienen incentivos económicos para operar con imparcialidad y garantizar la devolución del pago a los clientes, ya que suelen implicar a la comunidad de usuarios para recabar sus opiniones, y publican las decisiones adoptadas.

65 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' cit., p. 209.

La aparición de un ecosistema de derecho privado en la Dark Web es inevitable en la medida en que el Estado no valida los contratos ilegales.[66] Sin embargo, estos ecosistemas paralelos de derecho privado no son exclusivos de la Dark Net, sino que también han surgido, aunque a un nivel más localizado, en diferentes contextos tanto ilícitos como legales. Por ejemplo, se han publicado investigaciones sobre el autogobierno en entornos como las prisiones,[67] los barrios bajo control del IRA en Belfast,[68] las favelas de Río de Janeiro,[69] la esfera de los ladrones profesionales[70] y en el tráfico de drogas.[71] En estos entornos, la coerción violenta desempeña un papel crucial para la gobernanza de estos sindicatos del crimen organizado, imponiendo el funcionamiento del proceso de resolución de disputas y garantizando el cumplimiento de sus resultados.[72] Así pues, una distinción importante entre los sistemas de resolución de litigios en la Dark Web y la resolución de litigios tradicional en los bajos fondos de la delincuencia reside en la ausencia de amenaza real de violencia en el espacio digital.[73] Otra distinción crucial es el anonimato de los usuarios. De hecho, el objetivo de los sistemas de resolución de litigios en la Dark Web no es otro que aumentar la confianza entre los usuarios que desean realizar transacciones ilícitas con comerciantes anónimos, incluso con hackers y estafadores profesionales.

Más allá de las actividades delictivas, diferentes tipos de comunidades que operan dentro de los límites de la ley también han creado procesos de resolución de disputas para aplicar sus propias normas al margen de la ley estatal sin necesidad de recurrir a los Tribunales. Por ejemplo, en ámbito del matrimonio la Iglesia Católica y los judíos ortodoxos han desarrollado sus propios sistemas de resolución de litigios basados en sofisticadas normas sustantivas y procesales.[74] Estas instituciones no dependen de los tribunales estatales para hacer cumplir los resultados, ya que los usuarios se someten voluntariamente a estos sistemas autónomos de resolución de litigios que suelen tener sus propios mecanismos de ejecución.[75]

66 Dixit, A.: *Lawlessness and economics: Alternative Modes of Governance*, Princeton University Press, 2004.

67 Skarbek, D.: 'Governance and Prison Gangs' *American Political Science Review* 2011, vol. 105, num. 4, pp. 702–716.

68 Hamill, H.: *The Hoods: Crime and Punishment in Belfast*, Princeton University Press, 2011.

69 Arias, E., y Rodrigues, C.: 'The Myth of Personal Security: Criminal Gangs, Dispute Resolution, And Identity in Rio de Janeiro's Favelas' *Latin American Politics and Society* 2006, vol. 48, num 4, pp. 53–81.

70 Conwell, C., y Sutherland, E.: *The Professional Thief*, University of Chicago Press, 1956.

71 Reuter, P.: 'Systemic Violence in Drug Markets' *Crime, Law and Social Change*, 2009, vol. 52, num 3, pp. 275–289.

72 Véase also, Campana, P. y Varese, F.: 'Organized crime in the United Kingdom: Illegal Governance of Markets and Communities' *British Journal of Criminology,* 2018, vol. 58, num 6, p. 1393.

73 Dupont y Lusthaus, 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 218.

74 Broyde, M.: *Sharia Tribunals, Rabbinical Courts, and Christian Panels,* Oxford University Press, 2017, pp. 51–8, 151–3.

75 Bussani, M.: 'Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' *Cardozo Law Review,* 2019, vol. 40, p. 3148.

Podría decirse que estos sistemas de resolución de litigios, especialmente los de la Dark Web, se basan en un enfoque libertario y en una teoría de la justicia que contradice los principios democráticos liberales y el Estado de Derecho. No sólo porque su uso permite la proliferación de actividades delictivas, sino también porque el proceso de resolución de disputas no ofrece garantías procesales, ni asegura una supervisión judicial sujeta a una revisión en apelación como se requiere en cualquier Estado de Derecho. En consecuencia, los sistemas de resolución de litigios en la Dark Net plantean una serie de riesgos en términos de equidad procesal y sustantiva porque no están regulados ni supervisados y, por tanto, no pueden garantizar que sean imparciales o justos. Además, un reto añadido en los sistemas de resolución de litigios que operan en la Dark Web es la falta de transparencia, que se ve aumentada por el anonimato de las partes, y la falta de claridad de las pruebas necesarias para sustentar una demanda con éxito.

Por el contrario, en este estudio se ha observado que los adjudicadores tratan de impulsar la transparencia y la legitimidad en el proceso de resolución de litigios consultando a la comunidad del mercado y, lo que es más importante, tienen incentivos económicos para actuar de forma imparcial y de acuerdo con las normas del mercado y las condiciones contractuales de la transacción, ya que, de lo contrario, los usuarios irían a otros mercados de la competencia. En consecuencia, la herramienta de resolución de litigios en la Dark Web ofrece una opción de reparación accesible e imparcial, que cumple conalgunos requisitos del Estado de Derecho, ya que los litigios se resuelven de conformidad con el contrato y las normas del mercado, y el proceso de resolución de litigios está dirigido por terceros imparciales que reflejan la diversidad de las comunidades en las que operan. [76]

En una línea similar, a medida que las normas sustantivas y procesales van surgiendo orgánicamente para abordar las características idiosincrásicas de los litigios en la Dark Web, es posible trazar una línea comparativa con la *lex mercatoria* que surgió como un importante cuerpo de derecho mercantil para los comerciantes en Europa durante la época medieval, mitigando así los retos para los comerciantes internacionales a la hora de cumplir con las costumbres locales. De forma comparable al desarrollo de la *lex mercatoria* (e incluso del *common law* inglés),[77] los procesos de resolución de litigios en la Dark Web están evolucionando como sistemas basados en costumbres y prácticas internacionalmente aceptadas, que ahora se encuentran cada vez más codificadas como parte de las normas de los mercados de la Dark Net. De ahí que el entorno en línea y su naturaleza transfronteriza hayan dado lugar al desarrollo de estas medidas de autogobierno.

76 Véase 'What Is Rule of Law?', *World Justice Project*, www.worldjusticeproject.org/about-us/overview/what-rule-law. Véase Tushnet, M., 'Critical Legal Studies and the Rule of Law', en Loughlin, M. y Meierhenrich, J. (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge University Press, 2021, pp. 3-22.

77 Baker, JH: "The Law Merchant and the Common Law" *Cambridge Law Journal,* 1979, vol. 38, num 2, p. 295.

Aunque la legislación estatal se aplica para regular ciertos aspectos de Internet, como la protección de datos y las leyes de propiedad intelectual, la mayoría de las relaciones, especialmente en las redes sociales, se rigen por los términos y condiciones de estas redes y mercados. Como observa Bussani, "la legitimidad de esta gobernanza reside en el ideal de autodeterminación y autorregulación, y estos mundos virtuales crean su propia ley, que casi nunca se aplica a través de los canales legales oficiales".[78] A pesar de que estos espacios operan dentro de los límites de la legislación estatal, la aplicación de las normas y decisiones corre a cargo, en gran medida, de los administradores de estos espacios, que refuerzan sus propias concepciones contextuales del comportamiento aceptable.[79] Estas normas se denominan a veces *lex informática* para englobar la autorregulación desarrollada por la comunidad de usuarios de Internet como parte de sus normas y reglas habituales. Así pues, la *lex informática* puede considerarse parte de la regulación del ciberespacio[80] y una extensión de la *lex mercatoria*.[81]

De forma similar a cómo surgieron la lex mercatoria y la *lex informatica*, la autonomía social y económica de la Dark Web está contribuyendo a la generación de normas internas para regular sus transacciones ilícitas, que enfatizan la libertad contractual, evitan deliberadamente los tecnicismos legales y deciden los casos sin referencias a la ley, basándose en las reglas del mercado, las condiciones contractuales de la transacción y en lo que el juzgador considera justo y razonable en las circunstancias específicas del caso (es decir, basándose en el principio equitativo de *ex aequo et bono*). Así pues, este ámbito social autónomo cuenta con un ecosistema de derecho privado propio que funciona de forma paralela e independiente del Derecho estatal. Y lo hace de un modo más efectivo y accesible que el funcionamiento de los tribunales estatales a los que las partes con disputas sobre transacciones ilicitals no pueden acudir, aunque con una merma de garantías procesales.

Los procesos de resolución de disputas en la Dark Web siguen el modelo de justicia informal que ha caracterizado a los procesos extrajudiciales (*Alternative Dispute Resolution* o *ADR)*. Estos procesos se caracterizan por su estructura no burocrática basada en procesos *ad hoc* que operan en mercados virtuales relativamente pequeños.[82] Los procesos son accesibles a los usuarios del mercado sin necesidad de intermediarios legales, como abogados, que se requieren en los

78 Bussani, Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' cit., p. 3156.

79 Ibid, p. 3157. Véase, Suzor, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' Mercer L. Rev., 2012, vol. 63 p. 523, 530.

80 Johnson, D. y Post D.: "Law and Borders: The Rise of Law in Cyberspace" *Stanford Law Review,* 1996, vol. 48, num. 5, p. 1367.

81 Wright, A. y De Filippi, P.: 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 marzo 2015). Véase https://ssrn.com/abstract=2580664.

82 Palmer, M., y Simon, R.: *Dispute Processes - ADR and the Primary Forms of Decision-making*, 3rd ed., Cambridge University Press, 2020, p. 18.

procesos formales de resolución de disputas como el arbitraje o la via jurisdiccional. El proceso de resolución de conflictos está diseñado y dirigido por administradores del mercado con poca o ninguna formación en resolución de conflictos, y mucho menos en Derecho. Además, las normas sustantivas se elaboran a partir de los valores de la comunidad y la libertad contractual, en lugar de basarse en la legislación estatal. Del mismo modo, las normas de procedimiento son en gran medida imprecisas, no escritas y flexibles.

Los procesos de resolución de litigios en la Dark Web, al igual que los de los tribunales nacionales y en los sistemas regulados de ADR, como en el caso de los *ombudmen* y defensores del consumidor, tienen una función pública que va más allá de ofrecer reparación a los demandantes particulares. Su principal objetivo es promover la confianza dentro de la comunidad del mercado, y lo consiguen, entre otras cosas, disuadiendo comportamientos fraudulentos, evitando la aparición de nuevas disputas, buscando justicia e igualdad para la comunidad y expresando una identidad comunitaria. Estos objetivos también se encuentran en los mercados legales de Clear Web, ya que buscan igualmente aumentar la confianza de los usuarios y fomentar el comercio. Una investigación empírica en eBay descubrió que ofrecer un proceso de resolución de litigios aumenta la lealtad de los usuarios, incrementando incluso la actividad económica de quienes pueden resolver sus disputas de forma expeditiva.[83] Sin embargo, una peculiaridad de los foros de resolución de disputas de la Dark Net es que los administradores del sitio suelen leer las disputas y, al mismo tiempo que las resuelven, obtienen información sobre las causas de las mismas, de modo que pueden identificar mecanismos para evitar que surjan en el futuro, introduciendo cambios en el diseño del Mercado. Por ejemplo, un sub-foro del Archetyp Market afirma que el moderador detectó que los compradores frecuentemente no podían iniciar reclamaciones porque se les pasaba el breve plazo para hacerlas, por lo que el administrador añadió una función que advertía con antelación a los compradores del plazo límite para iniciar un litigio.

Mientras que los tribunales nacionales, e incluso los procesos ADR, no suelen proporcionar un acceso efectivo a los usuarios más pobres o marginados,[84] podría argumentarse que los procesos de resolución de litigios en la Dark Net pueden ser más eficaces y accesibles para todos los usuarios. Esto se debe a que es más probable que estos usuarios tengan mayores conocimientos informáticos que los consumidores medios, ya que necesitan estos conocimientos para procesar una

83 Rule, C.: 'Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution' *University of Arkansas Little Rock Law Review,* 2012, vol. 34, pp. 767–777.

84 Véase Galanter., M. y Krishnan, J.: 'Lok Adalats and Legal Rights in Modern India', en E. Jensen y T. Heller (eds) *Beyond Common Knowledge: Empirical Approaches to the Rule of Law,* Stanford University Press, 2003, pp. 96–127.

transacción (es decir, desde acceder a la Dark Net hasta pagar con criptomoneda y cifrar sus datos personales). Es posible que a estos usuarios no les resulte difícil participar en el proceso de resolución de litigios, que básicamente requiere que expliquen su reclamación y adjunten capturas de pantalla en un entorno más bien informal. Sin embargo, como las disputas están relacionadas con transacciones ilícitas, es posible que usuarios, a pesar de operar de manera anónima, decidan no presentar una reclamación, especialmente cuando sus reclamaciones se comparten en un sub-foro público. Así pues, las herramientas para evitar disputas también desempeñan un papel crucial como complemento de los sistemas de resolución de disputas.

Aunque los mecanismos de resolución de disputas en la Dark Web no distinguen entre casos penales y civiles, como se ha señalado en la sección anterior, varios mercados han desarrollado dos sistemas separados, uno para procesar las reclamaciones de comportamiento fraudulento, y otro para resolver disputas cuando no hay pruebas claras de fraude. Mientras que el principal remedio y objetivo de las listas de estafadores es eliminar a los vendedores deshonestos prohibiendo su participación en el mercado, el remedio más común en el proceso de resolución de disputas es la reasignación del pago de la transacción, o parte de él, a la parte ganadora. La ejecución de una decisión puede ser llevada a cabo por el administrador cuando tiene el control sobre la criptomoneda, e incentivando el cumplimiento voluntario para evitar la expulsión del mercado. Sin embargo, este tipo de sistema no es infalible, ya que las decisiones no siempre pueden autoejecutarse, especialmente cuando el demandado desaparece del mercado y las partes no han utilizado un sistema de custodia, o cuando el pago de la transacción ya se ha transferido al vendedor.

VI. CONCLUSIÓN.

La resolución de controversias contractuales, sean o no sobre transacciones ilícitas, no son monopolio del Estado. Sin embargo, el Estado no ejecutará las decisiones relativas al comercio ilegal. Como resultado, los mercados en la Dark Net han desarrollado sus propias herramientas que buscan evitar la aparición de disputas a través del uso de advertencias sobre usuarios fraudulentos, requiriendo el pago de una fianza a los vendedores y administrando un sistema de reputación para los vendedores. Cuando surgen disputas y las partes no pueden llegar a un acuerdo amistoso, generalmente confían en el servicio de custodia (*escrow*) y en el administrador del mercado para resolver las disputas. La comunidad del mercado también juega un papel importante, a menudo informando a los usuarios sobre las posibilidades de éxito de la reclamación y fomentando la resolución colaborativa de los conflictos.

Hasta la fecha la investigación de la resolución de disputas dentro de la Dark Web ha sido extremadamente escasa. Estos mecanismos, junto con sus sistemas de gobierno, han logrado aumentar la confianza de los usuarios en estos mercados ilícitos, lo que permite que miles de personas desconocidas participen en transacciones ilegales entre sí. Por lo tanto, funciona como una herramienta eficaz para generar y gestionar la confianza entre los usuarios, ayudando a expandir la actividad delictiva de estos mercados.

De manera similar a cómo surgió la *lex mercatoria* a través del establecimiento de tribunales arbitrales ubicados a lo largo de las principales rutas comerciales europeas, los procesos de resolución de disputas se están erigiendo en los mercados digitales, tanto legales como ilegales. Además, el servicio de custodia suele garantizar la ejecución de las decisiones. Como primer análisis legal académico de los métodos de resolución de disputas empleados en la Dark Web, el presente estudio ha pretendidodo mejorar nuestro conocimiento sobre un ecosistema de derecho privado que está emergiendo en la Dark Web con el objetivo de eliminar a los usuarios fraudulentos y brindar reparación a la comunidad de usuarios. Dichos procesos podrían extenderse al comercio electrónico legal en la medida en que éste empiece a aceptar pagos en criptomonedas o utilice sistemas de depósitos (*escrows*).

BIBLIOGRAFÍA

Afilipoaie, A., y Shortis, P.: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' *Global Drug Policy Observatory, Situation Analysis*, 2015.

Aminuddi, M., Zaaba, Z., Samsudin, A., Zaki, F. y Anuar, N.: 'The rise of website fingerprinting on Tor' *Journal of Network and Computer Applications,* 2023.

Analyst1, 'Dark Web – Justice League' (*Analyst1,* 2021) https://analyst1.com/dark-web-justice-league/

Arias, E., y Rodrigues, C.: 'The Myth of Personal Security: Criminal Gangs, Dispute Resolution, And Identity in Rio de Janeiro's Favelas' *Latin American Politics and Society* 2006, vol. 48, num 4, pp. 53–81.

Baker, JH: 'The Law Merchant and the Common Law' *Cambridge Law Journal,* 1979, vol. 38, num 2, p. 295.

Bisson, D., 'How a Cyber Criminal Justice System Resolves Disputes' (*Security Intelligence,* 26 enero 2022) https://securityintelligence.com/news/cyber-criminal-justice-system-resolves-disputes/.

Bracken, B.: 'When Scammers Get Scammed, They Take It to Cybercrime Court' (*threat post,* 7 diciembre 2021) https://threatpost.com/scammers-cybercrime-court/176834/.

Broyde, M.: *Sharia Tribunals, Rabbinical Courts, and Christian Panels,* Oxford University Press, 2017, pp. 51–8, 151–3.

Bussani, M.: 'Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' *Cardozo Law Review,* 2019, vol. 40, p. 3148.

Campana, P. y Varese, F.: 'Organized crime in the United Kingdom: Illegal Governance of Markets and Communities' *British Journal of Criminology,* 2018, vol. 58, num 6, p. 1393.

Campana, P., y Varese, F.: 'Cooperation in criminal organizations: Kinship and violence as credible commitments' *Rationality and Society,* 2013, vol. 25, num 3, p. 265.

Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', Paper Series: No. 6 febrero 2015.

Choi, K-S and Lee, CS,: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' *Journal of Contemporary Criminal Justice* 2023, vol. 39, num. 2, p. 201.

Conwell, C., y Sutherland, E.: *The Professional Thief*, University of Chicago Press, 1956.

Croy, A.: *The Dark Web: The Covert World of Cybercrime*, Greenhaven Publishing LLC, 2018.

CyberSec_Sai, 'Did You Know Darkweb Has Its Own Courts and Justice System?' (*Medium*, 8 marzo 2023) https://medium.com/geekculture/did-you-know-darkweb-has-its-own-courts-and-justice-system-7ecfa25c46c8.

Cybersixgill, 'Trust on the Deep and Dark Web' (22 marzo 2022). Véase https://cybersixgill.com/news/articles/trust-on-the-deep-and-dark-web.

Davies, G.: 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers' *Journal of Criminal Law,* 2020, vol. 84 num 5, 408.

DeNicola, L.: 'What is the Dark Web?' *Experian - Cybersecurity* (12 mayo 2021). Véase https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

Dixit, A.: *Lawlessness and economics: Alternative Modes of Governance*, Princeton University Press, 2004.

DoingFedTime, 'Dispute Resolution Buyers vs Vendors – Deep Dot Dark Net' (27 noviembre 2022). https://www.youtube.com/watch?v=qwZvflkl-9c&t=12s.

Doyle, E.: *The Dark Web*, Greenhaven Publishing LLC, 2019.

Dupont, B., y Lusthaus, J.: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' *Social Science Computer Review,* 2021, vol. 40 num 4, p. 892.

Electronic Frontier Foundation, 'GCHQ Leak: A Potential Technique to Deanonymise Users of the TOR Network' UK Top Secret Strap1 Comint, OPC-M/TECH.B/61 (13 June 2011). Véase https://www.eff.org/document/20141228-speigel-potential-technique-deanonymise-users-tor-network.

Europol 'Cybercriminal Darkode Forum Taken Down Through Global Action' (15 julio 2015). Véase https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action

FINKLEA, K.: 'Dark Web', Congressional Research Service, 7-5700, R44101 (10 marzo 2017) p. 2. Véase https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf.

GALANTER., M. y KRISHNAN, J.: 'Lok Adalats and Legal Rights in Modern India', en E. JENSEN y T. HELLER (eds) *Beyond Common Knowledge: Empirical Approaches to the Rule of Law*, Stanford University Press, 2003, pp. 96–127.

HAMILL, H.: *The Hoods: Crime and Punishment in Belfast*, Princeton University Press, 2011.

HOFFMAN, H.: 'Facebook's Dark Web .Onion Site Reaches 1 Million Monthly Tor Users' (22 abril 2016). Véase https://www.inverse.com/article/14672-facebook-s-dark-web-onion-site-reaches-1-million-monthly-tor-users.

HOLLAND, A. et al.,: 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back' An HP Wolf Security Report' 2022. Véase https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf

HOLT, T. y LAMPKE, E., 'Exploring stolen data markets online: Products and market forces' *Criminal Justice Studies*, 2010, vol. 23, num. 1, pp. 33–50.

HOLT, T.: 'Exploring the social organisation and structure of stolen data markets' *Global Crime* vol. 2013, num. 14(2-3), pp. 155–174.

HP Wolf Security et al, 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape y How to Fight Back – An HP Wolf Security Report' (julio 2022). https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf p. 15.

JARDINE, E.: 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' *Global Commission on Internet Governance Paper Series,* 2015, vol. 21. Véase https://ssrn.com/abstract=2667711.

JOHNSON, D. y POST D.: "Law and Borders: The Rise of Law in Cyberspace" *Stanford Law Review,* 1996, vol. 48, num. 5, p. 1367.

KAPERSKY, 'Business on the dark web: Deals and regulatory mechanisms', 2023. Véase https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/03/10151223/Business-on-the-dark-web-deals-and-regulations.pdf?reseller=gl_regular-sm_acq_ona_oth__onl_b2b_securelist_lnk_sm-team.

KRISLOV, S., 'The Amicus Curiae Brief: From Friendship to Advocacy' *Yale Law Journal,* 1963, vol. 72, p. 694.

LUMMEN, DLM: 'Is Telegram the new Dark Net? A comparison of traditional and emerging digital criminal marketplaces' (MSc thesis, University of Twente 2023), p. 49.

LUSTHAUS, J.: *Industry of anonymity: Inside the business of cybercrime*, Harvard University Press, 2018.

MIREA, M., WANG, V., y JUNG, J.: 'The not so dark side of the Dark Net: a qualitative study' SJ, 2019, vol. 32, p. 105.

MUJEZINOVIC, D.: 'How to Police Hackers: Inside the Dark Web's Justice System' (*MakeUseOf,* 31 diciembre 2021) https://www.makeuseof.com/inside-dark-webs-justice-system/.

ORTOLANI, P.: 'Self-enforcing online dispute resolution: lessons from Bitcoin' Oxf. J. Legal Stud., 2016, vol 36, pp. 595–629.

PALMER, M., y SIMON, R.: *Dispute Processes - ADR and the Primary Forms of Decision-making*, 3rd ed., Cambridge University Press, 2020.

RAYMOND, A. y STEMLER, A.: 'Trusting Strangers: Dispute Resolution in the Crowd' *Cardozo Journal of Conflict Resolution,* 2014, vol. 16, p. 357.

REUTER, P.: 'Systemic Violence in Drug Markets' *Crime, Law and Social Change,* 2009, vol. 52, num 3, pp. 275–289.

RULE, C.: 'Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution' *University of Arkansas Little Rock Law Review,* 2012, vol. 34, pp. 767–777.

SKARBEK, D.: 'Governance and Prison Gangs' *American Political Science Review* 2011, vol. 105, num. 4, pp. 702–716.

Social Links, 'Top-10 OSINT and Cyber Security Stories of 2022' (*Social Links*, 28 diciembre 2022) https://blog.sociallinks.io/top-10-osint-and-cyber-security-stories-of-2022/.

STEVENSON, A.: 'It only took 2 weeks for the world's most dangerous hacking forum to get back online after the FBI shut it down' Insider (28 July 2015). Véase https://www.businessinsider.com/darkode-admin-returns-with-new-and-improved-hacking-site-2015-7?r=US&IR=T.

SUZOR, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' Mercer L. Rev., 2012, vol. 63 p. 523.

The Onion Router Project. Véase https://www.torproject.org/projects/torbrowser.html.en.

Tushnet, M., 'Critical Legal Studies and the Rule of Law', en Loughlin, M. y Meierhenrich, J. (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge University Press, 2021.

United Nations Office on Drugs and Crime, Global Overview – Drug Demand Drug Supply, Global Drug Report 2022. Véase https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_2.pdf.

US Department of Justice - Office of Public Affairs, 'Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"' (28 abril 2021). Véase https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

Vanian, J.: 'Online criminals have created their pseudo court system on the dark web' *Fortune* (7 diciembre 2021). Véase https://fortune.com/2021/12/07/online-criminals-court-system-dark-web-russian-hackers-ransomware/

Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading,* 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts;

White, G., y Archampong, P.: The Dark Web, Episode 7, Cybercrime Inc, Podcast, (8 febrero 2018).

Wixey, M.: 'The scammers who scam scammers on cybercrime forums: Part 1' (*Sophos*, 7 diciembre 2022) https://news.sophos.com/en-us/2022/12/07/the-scammers-who-scam-scammers-on-cybercrime-forums-part-1/.

Wright, A. y De Filippi, P.: 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 marzo 2015). Véase https://ssrn.com/abstract=2580664.

Yip, M. , Webber, C., Shadbolt, N.: 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing' *Policing and Society*, 2013, vol. 23, num. 4, pp. 516–539.