La confianza en los mercados oscuros.

Confidence in dark markets.

Fecha de presentación: Sepiembre 2019
Fecha de aceptación: Julio 2020

David Méndez Valiente.
Guardía Civil Española.

"Comercio electrónico"

Resumen

El comercio electrónico ya sea en la red profunda o en la superficie, al fin y a la postre es comercio, las interacciones entre vendedor y comprador están sujetas a la influencia de unos mismos factores, entre los que destaca la confianza. El presente artículo es una aproximación a como los proveedores de la red oscura tratan transmitir a los vendedores una imagen de confiabilidad. A ello, están colaborando terceras partes, erigidas como organismos acreditadores de la calidad y confiabilidad de los vendedores en la *dark net*. Una posible forma de actuar contra los mercados ilícitos de la red oscura por parte de las fuerzas de seguridad, puede ser influir sobre la percepción de confianza que los compradores tienen sobre los proveedores.

Palabras Clave

Comercio electrónico, transacciones electrónicas, dark web.

Abstract

E-commerce, whether in the deep web or on the surface, is ultimately commerce, the interactions between seller and buyer are subject to the influence of the same factors, among which trust stands out. This article is an approximation of how dark web providers try to convey an image of trustworthiness to vendors. To this, third parties are collaborating, erected as accrediting bodies of the quality and reliability of sellers on the dark net. One possible way to act against illicit dark web markets by law enforcement agencies may be to influence the perception of trust that buyers have in suppliers.

Keywords

Electronic commerce, transacciones electrónicas, dark web.

E-commerce en la dark web

El desarrollo y la globalización del comercio electrónico o *e-commerce*, ha permitido a las empresas alcanzar un mayor volumen de negocios con una reducción de los costos estructurales, lo que ha significado que grandes, medianas y pequeñas mercantiles puedan posicionarse en el mercado (Portilla y Taboada, 2020).

Según la Organización Mundial de Comercio (WTC) el *e-commerce* puede definirse como la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos. Los avances tecnológicos y el incremento de la accesibilidad a internet han agilizado el desarrollo de las transacciones comerciales. Por ello, el comercio electrónico es un dinamizador del proceso de encuentro entre oferta y demanda.

Las principales modalidades de comercio electrónico descritas por la WTC son: el realizado de empresa a empresa (B2B); el efectuado entre una empresa y los consumidores (B2C) Y el realizado entre una empresa y el gobierno (B2G). En España, durante el primer trimestre de 2020, la facturación del comercio electrónico ha aumentado en el primer trimestre de 2020 un 11,6% interanual hasta alcanzar los 12.243 millones de euros.

"Darknet o red oscura

El comercio electrónico presenta una serie de ventajas frente al comercio tradicional: mayor diversidad y disponibilidad de productos; mayor alcance geográfico; menor tiempo de compra; horario 24/7; no requiere desplazamiento físico al comercio; mayores alternativas de precio-calidad y mayor trazabilidad de clientes (DN Consultores, 2020). Estas características, han permitido al e-commerce posicionarse como un medio imprescindible para el desarrollo de una empresa.

Las características de las transacciones electrónicas de mercancías y servicios lícitos, son aplicables al *e-commerce* efectuado entre criminales. Al igual que sucedía con la migración progresiva de empresas y consumidores desde el mercado tradicional hacia el comercio electrónico. Los delincuentes están trasladando la arena de negocio a las tiendas virtuales hospedadas en la *dark web*, en los mercados de la red oscura es posible la compra-venta de mercancías ilegales (armas, drogas, pornografía infantil) o servicios para el crimen. Esta migración responde al esfuerzo adaptativo del ofertante a las tendencias del mercado y las necesidades de los clientes.

El ciber crimen es una evolución no una revolución, los fundamentos de la ciber criminalidad siguen siendo los mismos, ya que el ciber delito no es muy diferente de otras formas de delincuencia más tradicional (IOCTA, 2020). Con la expansión de internet y su uso, la delincuencia digital comenzó a direccionarse hacia un nicho de negocio delictivo especializado, dando lugar a un modelo de negocio conocido como *crime as a service* (CaaS). Si al comienzo de la era digital era necesarios ciertos conocimientos de seguridad informática para efectuar acciones criminales ahora sólo son necesarios una mínima motivación y un medio de pago (Soria, 2016). La subcontratación de las habilidades delictivas de cierta persona para llevar a cabo un delito siempre ha existido, sin embargo la misma naturaleza del negocio, los actores implicados y el medio virtual en que se realiza generan incertidumbre y desconfianza. Por este motivo, los mismos usuarios de la *dark web* han tratado de implementar herramientas que fomenten la confianza entre los anónimos proveedor y comprador.

La confianza en los mercados oscuros.

Creer que una persona actuará de una determinada forma en una situación concreta es una de las definiciones de confianza. Esta se establece a partir de las interacciones desarrolladas entre las personas, y hasta hace escaso tiempo, era a través de una interacción física la principal vía de desarrollo. Sin embargo, la tecnología además de permitir la expansión de mercados y posibilidades ha facilitado extender el círculo de confianza, las recomendaciones ya no vienen únicamente de personas con las que se tiene un contacto físico, si no que se pueden seguir los consejos de amigos de amigos o de desconocidos a través de un entorno virtual.

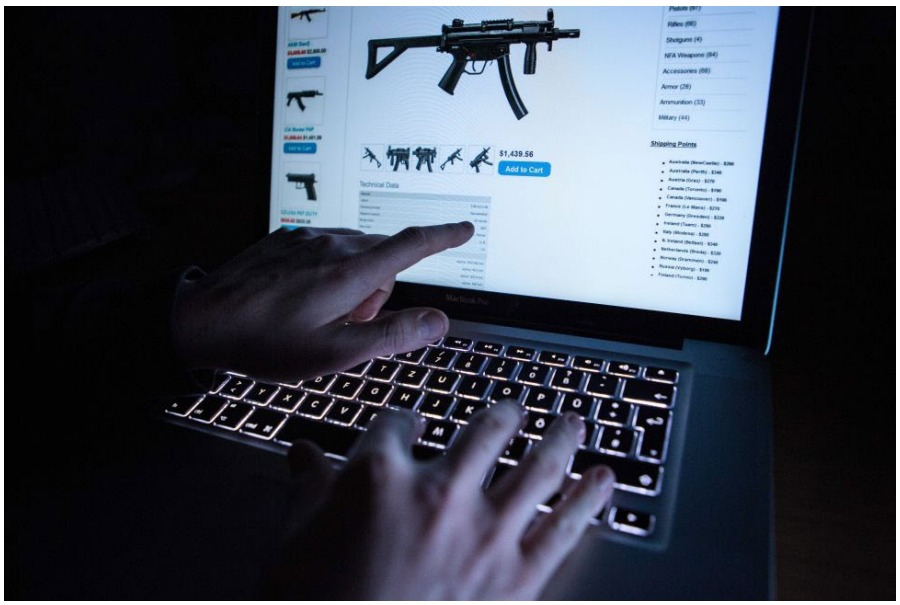
En la actualidad, las referencias e índice de confianza hacia un determinado vendedor no solo se dan entre los compradores en la *surface web*, por inverosímil que pueda parecer, en la *dark web* también se está creando confianza a pesar del manto de anonimato que cubre a los usuarios.

El acceso a la red oscura se realiza empleando un software especial de anonimización, generalmente el más empleado es "The Onion Router" (TOR). Junto con periodistas, organizaciones no gubernamentales que necesitan enmascarar su actividad en internet, la red oscura está poblada por delincuentes que ofrecen toda una variedad de artículos ilegales, desde drogas hasta armas pasando por el alquiler de sus conocimientos informáticos (Botsman, 2017). En un entorno real, estas personas serían calificadas cuanto menos como poco confiables, sin embargo en la *dark web* no solo están creando mercados eficientes con altas cuotas de transacciones, sino que están generando confianza y lazos estables en un entorno donde todos los actores son desconfiados.

El anonimato y la inexistencia de un marco regulatorio para las transacciones son características suficientes para despertar recelos y suspicacias para los compradores, pues eleva la posibilidad de ser estafados. Facilmente el vendedor podría sustituir la calidad de la sustancia comprada o no entregar el producto. No obstante, esto rara vez se produce, en la *dark web* es mucho más probable encontrar referencias sobre la confiabilidad de determinado vendedor, sobre la calidad de la mercancía se vende o sobre los servicios

que presta cierto proveedor.

Antes que se procediera a la detención de Ross Ulbricht y el cierre del mercado de productos ilícitos Silk Road, el FBI acreditó más de 50 compras de drogas de gran pureza a través de este servicio de intermediación (Frizell, 2015). Sin embargo, tener un buen producto es un elemento necesario pero no suficiente para generar confianza en el comprador. En este sentido los usuarios de la *dark net*, ante los crecientes problemas estafa y phising que rodeaban los sitios de negocios ".onion" demandaron a la comunidad la creación de un servicio que proporcionara enlaces legítimos y verificables. De entre las diferentes opciones creadas, destaca Dark.fail quien se ha posicionado como uno de los mejores sitios independientes de la *dark web* para los enlaces de mercado, en este *site* priman los intereses de los usuarios. Cuando surge un mercado nuevo en la red profunda, Dark.fail analiza las características del sitio y las comparte con la comunidad tratando de aportar cierto nivel transparencia y objetividad, indica principales productos a la venta, métodos de pago aceptados, cantidad de proveedores. Por ejemplo, sobre "Monopoly Market", lugar de transacciones de estupefacientes, Dark.fail señala que es un mercado centrado en la calidad sobre la cantidad que *"únicamente permite la entrada a los proveedores más confiables, 132 están allí actualmente. Se aceptan diseños elegantes, tutoriales amigables, bitcoin y monero".*



El conocimiento obtenido hasta la fecha sobre las transacciones realizadas en la web oscura parece indicar que los proveedores en los ciber mercados ilegales son buenos comerciantes, tratan satisfacer al cliente y lograr su retención a través de la venta de un producto de calidad, entregado discretamente y certificado a través de revisiones en línea.

El mercado en la *dark web* no deja de ser un espacio en el que personas se conectan con otras personas, en palabras de Amman (2020) "El ciber crimen trabaja en cierta forma como la economía legal, tiene unos actores que tratan de innovar pero también hay otros actores que piensan 'si ha funcionado los últimos 10 años porque cambiar el equipo ganador'". Por lo tanto, los mercados de la red oscura no son más que espacios de transacciones humanas que reflejan como la tecnología ha facilitado una nueva forma de construir relaciones de confianza. El ciber crimen no es una revolución, si no tan solo una evolución (IOCTA, 2020) de las formas y métodos de delincuencia tradicional, pero sobre todo de las mismas dinámicas y principios que fundamentan las relaciones humanas digitales.

En la *Surface web* un vendedor en ebay, Aliexpress, Amazon o un proveedor de Booking se preocupa por la satisfacción del cliente y como esta afecta a la reputación online de su marca. Tratando de ser transparente y mostrar la calidad de su servicio, en su espacio de venta tratará de facilitar información como: el nombre o seudónimo, fecha de registro o las transacciones realizadas. Los proveedores en la *dark web* incluyen también estos datos como argumentos sobre por qué son una buena opción de compra y los amplían añadiendo políticas de reembolso, opciones de envío y descripciones sucintas sobre qué medidas emplean para evitar la detección de su paquetería. Es decir que los vendedores de la red oscura, tratan de hacer esfuerzos reales para demostrar la confiabilidad.

El proveedor de la *dark web* quiere transmitir confiabilidad a los potenciales clientes, para ello emplean estrategias derivadas del marketing tradicional. Para captar compradores diseñan programas de fidelización, ofertas especiales, descuentos por volumen e implementan garantías de reembolso. En su afán por construir marca, los proveedores de la red oscura pueden llegar a adjetivar sus productos orgánicos o de comercio justo. O recurren a terceros imparciales para que evalúen la calidad de su producto.

Con respecto a este último punto, cabe destacar la función que realiza el laboratorio español Energy Control, que se ha alzado como referencia a nivel mundial en la acreditación de la calidad de drogas ilegales. El funcionamiento es sencillo, un proveedor o cliente que quiere saber la calidad de su producto con vistas a publicitarlo en la *dark web*, envía anónimamente una muestra de la sustancia, un nombre del producto, el seudónimo del vendedor y un email al que puedan remitir los resultados. Una vez realizados los análisis los resultados se remiten al correo electrónico facilitado en PDF y se publicitan en la red oscura para conocimiento de la

comunidad. Básicamente lo que se transmite a los potenciales compradores es que X producto vendido por Y tiene un nivel de calidad Z, y que estos datos están avalados por una certificadora independiente.

Este servicio de pruebas que tiene un coste de entre 30€ y 170€ abonados en Bitcoins (Energy Control, 2020), existe en una zona gris legal que permite a este organismo desarrollar su labor (Cox, 2015). Las personas propietarias del laboratorio están acreditadas para experimentar y manipular drogas, pero Energy Control no tiene este permiso.

DarkNet Market Avengers es un sitio de la red oscura en el que se publican los resultados aportados por Energy Control, se incluye calidad del producto, nivel de pureza, toxicidad y proveedor. El principal resultado de este sistema es que los estafadores y aquellos proveedores de productos de baja calidad son expulsados con relativa rapidez de los mercados, ya que toda la comunidad aporta y es conocedora de las circunstancias de determinado producto y su vendedor.

Por este motivo, los proveedores no solo trataran de ofrecer muestras gratuitas, políticas de igualación de precios, campañas promocionales, sino que a través de la calidad del producto intentarán establecer su reputación en el mercado, se ha detectado que las drogas compradas en la *dark web* tienen mayor grado de pureza y calidad que las obtenidas en el mercado tradicional (Energy Control, 2020).

Pero si ya se ofertan productos de calidad, se garantiza el anonimato, se permite los pagos en criptomoneda ¿es esto suficiente para asegurar el éxito futuro de los mercados en la red oscura? No, el verdadero secreto del éxito de los espacios de venta de la *dark net* es su excelente servicio de atención al cliente (Bartlett, 2014).

El servicio de atención al cliente de los distintos proveedores se evalúa a través de las calificaciones de los compradores, una vez recibida la mercancia se le pide que deje una valoración de la transacción y el producto. Crhistin (2012) analizó los comentarios de compradores realizados en Silk Road antes de su cierre, el resultado fue que el 97,8% de las reseñas fueron positivas. Lo que puede ser un indicador de lo notablemente bien que funciona el mercado de la red oscura la mayor parte del tiempo. Los mecanismos de revisión al fin y al cabo son un mecanismo de control social responsable, ya que tienen el potencial de hacer que las personas se comporten mejor.

Existe un incentivo claro para que los proveedores proporcionen constantemente el producto y el servicio que prometen: los distribuidores con las mejores críticas llegan a la cima (Botsman, 2017). Dado que no se pueden eliminar los comentarios, existe un registro del historial de comportamiento de los compradores, por lo que el comprador proyectará la conducta pasada del proveedor hacia el futuro y declinará la transacción si los registros anteriores son negativos. La reputación al fin y al cabo es una medida de confiabilidad. Los clientes eligen entre diferentes opciones en parte por la reputación de los vendedores, y anima a estos a ser dignos de confianza para construirla, de modo que los que proveedores que no son dignos de confianza son eliminados de los mercados.

Además de la problemática de cómo generar la confianza entre los anónimos proveedor y cliente, los mercados de la red profunda se han encontrado con turbulencias derivadas de su propia volatilidad y de la represión de las autoridades. Esto ha supuesto que los sitios de mercado en la *dark web* sean muy inestables. Según el informe de Trend Micro (2020) tras la imposición de medidas por las autoridades en *sites* como Valhalla o DeepDotweb los usuarios experimentaron un mayor nivel de incertidumbre sobre la seguridad de la infraestructura de la red oscura. Lo que produjo una desaceleración en la actividad de ventas.

Muchos usuarios de los mercados de la *dark net,* tras estas acciones de las autoridades, incrementaron las medidas para garantizar su anonimato lo que ha degenerado en un aumento de las *scam exit*, estafas de salida en las que un mercado web cierra de repente y roba el dinero depositado por los clientes (Sentilecto, 2020).

Esta falta de confianza en los mercados de la red oscura ha generado la necesidad de crear espacios en los que visualizar la reputación de los proveedores a través de la búsqueda de su *nickname* y las huellas digitales PGP.

Toda esta problemática ha obligado a que los administradores de la red oscura a implementar nuevos atributos de seguridad para las transacciones y así generar mayor confianza entre los usuarios, tanto a proveedores como potenciales clientes, así han aplicado sistemas de firma múltiple en criptomoneda, comisiones mensuales por servicio en lugar de comisiones por transacción, liberación del pago tras confirmación de recepción del producto por el comprador.

Sin embargo la integridad no puede ser algo fácilmente asociable a los mercados en la *dark web* en los que las transacciones a realizar son entre individuos anónimos y de productos ilegales o empleados para cometer hechos delictivos. Sin embargo, los foros de comercio de la red oscura tienen un fuerte sentido de

comunidad con unas normas claras y una cultura propia, que regulan el sistema de mercado expulsando a aquellos que no son de fiar.

"Organización Mundial de Comercio (WTC)"

Conclusiones.

La evolución observada en los mercados situados en la *dark web* y preferencias observadas en los usuarios de estas plataformas permiten afirmar que la red oscura se está convirtiendo para los delincuentes con un producto a ofertar (drogas, armas, pornografía infantil, CaaS) en un importante canal de venta, que cada vez acapara más cuota de transacciones con respecto a los métodos tradicionales de venta. Los delincuentes han observado que los criptomercados son una oportunidad de negocio en el que reducen la cadena de suministro, al tiempo que minimizan riesgos y comportamientos asociados a determinados delitos, en especial al tráfico de drogas y armas asociados al comercio delictivo tradicional. La ubicuidad y permanencia de estos espacios de transacción representan para los proveedores de material ilícito, alcanzar un mayor número de potenciales clientes a quienes proporcionar una mayor disponibilidad de productos ilícitos de mejor calidad, lo que redunda en un aumento de beneficios.

Estos sistemas de comercio en la *dark web* funcionan al fin y al cabo por que los clientes tienen la capacidad de votar y valorar los servicios que los proveedores les facilitan. La tecnología permite que los compradores puedan hacer que los vendedores rindan cuentas por sus productos y servicios, de forma que solo aquellos que se perciban como confiables sobrevivirán en los efímeros mercados de la red oscura. En definitiva el comercio electrónico en a *dark web* no es más que comercio electrónico, y como tal está sujeto a la influencia que la reputación ejerce en los actores implicados. Es por ello, que la elaboración por parte de las autoridades de los países para implementar acciones de influencia en la reputación de los mercados y proveedores en la red oscura, puede ser un medio relativamente económico y efectivo para alterar este ecosistema, si se genera mayor incertidumbre sobre la confiabilidad de los proveedores, estos tendrán mayores dificultades para colocar su producto.

En este sentido, puede ser efectivo fiscalizar las acciones de laboratorios como Energy Control, cuanto menos regular aspectos relevantes como identificación plena del solicitante del servicio de análisis o impedir que puedan abonarse los servicios prestados por criptomoneda puede ser un modo de dificultar este tipo de actividades de dudosa utilidad. Al margen del supuesto beneficio que pueden tener sus aportaciones como parte integrante del Sistema Español de Alerta Temprana sobre Drogas, no se debe olvidar que su principal motivación es facilitar al consumidor información sobre la composición de las sustancias que va a tomar, así como recibir un asesoramiento individualizado sobre pautas de uso de menor riesgo (Energy Control, 2020), para ello realizan campañas en defensa del uso recreativo de las drogas argumentando que los efectos nocivos de las mismas no son tanto por su abuso como por su composición. A la larga, la actividad certificadora de laboratorios como este, contribuyen a afianzar la posición de mercado de determinados vendedores de drogas en la dark web, lo cual de un modo directo o indirecto confronta con los intereses mayoritarios de la sociedad en general y con las acciones de las Fuerzas y Cuerpos de Seguridad en particular.

Referencias

Amman, P. (2020). Launch of the IOCTA 2020. Europol. La Haya, online. Recuperado de https://youtu.be/fTzmglycoUE

Bartlett, J. (2014) The Dark Net: Inside the Digital Underworld. UK: Heinemann

Botsman, R. (2017). How Darknet Sellers Build Trust. Nautilus. Recuperado de: http://nautil.us/issue/55/trust/how-darknet-sellers-build-trust. Consulta 13 de octubre de 2020.

Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Proceedings of the 22nd International Conference on World Wide Web. Recuperado de: https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf

Cox, J. (27 de marzo de 2015). Inside the Deep Web Drug Lab. Blackchannel. Recuperado de https://medium.com/backchannel/inside-the-deep-web-drug-lab-9718cd0fe504. Consulta el 8 de octubre de 2020.

DN Consultores. Comercio electrónico y microempresa (2020). Recuperado de: http://dnconsultores.com/informe/inf2011ce/. Consulta el 09 de octubre de 2020.

Organización Mundial del Comercio (WTO). Entender la OMC: Cuestiones Transversales y Cuestiones nuevas – Comercio Electrónico. Recuperado de: https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm. Consulta el 10 de octubre de 2020.

Portilla, F. y Taboada, A. L. (4 de junio de 2020). Los Delitos Informáticos en Tiempos de e-commerce. IUS 360. Recuperado de: https://ius360.com/publico/penal/los-delitos-informaticos-en-tiempos-de-e-commerce-fernando-portilla-ana-lucia-taboada/

Searchlight Security. Dark.fail. https://www.slcyber.io/wiki/article/dark-fail#:~:text=Dark.-fail,links%20to%20these%20onion%20sites.

Sentilecto (8 de junio de 2020). Las fuerzas del orden comienzan a hacer que los criminales duden de la dark web. Entretenimientobit. Recuperado de: https://entretenimientobit.com/crypto/las-fuerzas-del-orden-empiezan-a-hacer-que-los-criminales-duden-de-la-dark-web/ Consultado el: 10 de octubre de2020