ISSN: 1390-4299
1390-3691

No. 21

URVIO

Revista Latinoamericana de Estudios de Seguridad

Inteligencia militar

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Diciembre 2017

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2017 - No. 21

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del *Master Journal List de Thomson Reuters*.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales-Región Andina y América Latina-FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- JournalTOCS. Base de datos.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- Google académico. Buscador especializado en documentación académica y científica.
- Directory of Research Journals Indexing (DRJI). Directorio.

FLACSO ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 21, diciembre de 2017
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

Envío de artículos
revistaurvio@flacso.org.ec

FLACSO, sede Ecuador
Casilla: 17-11-06362
Dirección: Calle Pradera E7-174 y Av. Diego de Almagro. Quito, Ecuador
www.flacso.edu.ec
Telf.: (593-2) 294 6800 Fax: (593-2) 294 6803

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - diciembre 2017 - No. 21

Tema central

Misceláneo

Reseñas

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - diciembre 2017 - No. 21

Central topic

Miscellaneous

Books reviews

DOI: http://dx.doi.org/10.17141/urvio.21.2017.2824

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 21, Quito, diciembre 2017, pp. 191-206
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Narcotráfico en la Darkweb: los criptomercados

Illicit Drug Trafficking on the Darkweb: Criptomarkets

Luis Ignacio García Sigman[1]

Fecha de recepción: 1 de mayo de 2017
Fecha de aceptación: 11 de octubre de 2017

Resumen

En el marco del creciente interés y preocupación generada por el narcotráfico a través de Internet, el presente artículo se propone presentar, de manera sistemática y sucinta, los principales rasgos del tráfico ilícito de drogas en la Internet oscura. Para hacerlo, el trabajo se dividirá en dos partes. La primera, más breve, dedicada a distinguir los diferentes niveles de Internet. La segunda, más larga, enfocada en presentar los principales rasgos de los criptomercados. En particular, se intentarán describir, en esta sección, las tecnologías de seguridad y los mecanismos que usan para generar confianza en los compradores y vendedores; sus potencialidades y límites; su impacto en los diferentes niveles del tráfico ilícito de drogas; los tipos y las cantidades de estupefacientes que se comercializan en ellos; el perfil de los compradores y de los vendedores; y también las estrategias concebidas por los estados para restringirlos. La consecución de dichos propósitos supondrá que se tomen como referencia los trabajos más relevantes que, hasta el momento, se escribieron sobre el tema.

Palabras clave: criptomercados; drogas; Internet oscura; narcotráfico.

Abstract

In the context of the growing interest in and concern about drug trafficking carried out over the internet, this article aims to describe, in a systematic and succinct fashion, the principal characteristics of the illegal drug trade on the dark web. To this end, the article will be divided into two sections. The first, shorter section, will distinguish between the different "levels" of the internet. The second, longer section, will focus on describing the principal characteristics of these crypto-markets. As regards these sorts of dark web markets, this section will detail the security measures and mechanisms that they utilize to generate trust among buyers and sellers; their capabilities and limits; their impact on various levels of the illegal drug trade; the types and quantities of narcotics that are sold on them; the profile of the buyers and sellers who use them; and also the strategies designed by states to limit them. The achievement of said objectives presupposes that the most relevant and up-to-date work written about this subject will be used as reference material.

Keywords: criptomarkets; drug; dark web; drug trafficking.

1 Licenciado en Ciencia Política por la Universidad de Belgrano, Magíster en Periodismo por la Universidad de San Andrés, Doctor en Ciencia Política por la Universidad de Belgrano y Posdoctorado por la Universidad Nacional de Córdoba. Correo: nachogarciasig@gmail.com

Introducción

En menos de tres décadas, se incrementó significativamente el número de usuarios de Internet. Las conexiones mejoraron en términos de la velocidad y del volumen de información que posibilitan intercambiar, y también surgieron múltiples dispositivos móviles que permiten a las personas conectarse a la red. Estas tres tendencias han tenido un significativo impacto en la dinámica y en la lógica de los negocios lícitos y, lógicamente, también en la de los ilegales. Dentro del tráfico ilícito de estupefacientes no ha habido excepción (Mounteney *et al.* 2016, 13). Tal como se verá, la comercialización ilícita de estupefacientes *on line* se realiza tanto en el plano superficial de la *web* como en el más profundo. En particular, los mercados de drogas ilícitas que funcionan en la *Dark Web* son los que, últimamente, han despertado mayores niveles de curiosidad, interés y preocupación en cada vez más actores.

En el marco del interés y la preocupación generada por esta problemática, el presente artículo se propone presentar, de manera sucinta, los principales rasgos del tráfico ilícito de estupefacientes en la *web* oscura. Así, la consecución de este propósito supondrá que este trabajo, que se construyó a partir de una revisión de parte de la literatura de referencia sobre la materia, se estructure en dos partes. En la primera, se indicarán los rasgos de los tres niveles de la *web* (superficial, profundo y oscuro); y, en la segunda, se presentarán algunos de los principales rasgos de los criptomercados, es decir, los mercados virtuales que funcionan en la web oscura y en los que se venden –en mayor medida, pero no solo– drogas ilícitas.

Niveles de internet y tipos de mercados de drogas ilícitas

Habitualmente, la mayoría de las personas que navegan en la *web* no saben que resulta posible distinguir tres planos en ella. En primer lugar, la *web* superficial que es la porción de Internet cuya información está indexada por los motores de búsqueda y que es accesible a través de los navegadores tradicionales (Internet Explorer, Google Chrome o Firefox) (EMCDDA 2016, 135; Kruithof 2016, xxxiii). En segundo lugar, la *web* profunda, que es la parte de Internet cuyos contenidos no pueden ser indexados por los buscadores (información y bases de datos que están protegidas por contraseñas y que pertenecen a agencias gubernamentales, bibliotecas o universidades; contenido dinámico y documentos en formatos no indexables) y a los que también puede accederse utilizando los navegadores clásicos (EMCDDA 2016, 136; Kruithof 2016, xxxiv; Chertoff y Simon 2015, 1).

Para tomar conciencia de la magnitud de esta parte de la *web*, puede señalarse que es 500 veces más grande que la superficial y también que, por la magnitud de información que almacenan, los 60 sitios más importantes de la *deep web* son 40 veces más grandes que toda la *web* superficial (Chertoff y Simon 2015, 1; Sui *et al.* 201, 6). En tercer lugar, la *web* oscura, que es una pequeña parte de la web profunda que, del mismo modo que ella, tampoco está indexada por los motores de búsqueda, pero que, a diferencia de aquella, es restringida, es decir, no se puede acceder a ella con los navegadores clásicos. Así, la *web* oscura es una porción de la *web* profunda que se ocultó intencionalmente y a la que solo puede llegarse a través de programas tales como, por ejemplo,

el *Tor Browser* que, a su vez, permite acceder a la *red Tor* (EMCDDA 2016, 136; Kruithof 2016, xxxiii; Chertoff y Simon 2015, 1-3).

Antes de continuar con el siguiente tema de esta sección, se considera importante señalar que la *Dark web* no es intrínsecamente mala, que no todo aquel que ingresa a ella es un delincuente ni que todo lo que, en su marco, se realiza es malo, ilegal o reprochable. Es necesario tener claro que la *web* oscura tiene, desde el punto de vista de la naturaleza y de los propósitos que tienen las actividades que se realizan en su seno, un carácter dual o ambivalente. Por un lado, el anonimato que en el marco de la *web* oscura puede alcanzarse, configura una herramienta que, lógicamente, resulta conveniente para la ejecución de actividades criminales y que, por lo tanto, es aprovechada, entre otros, por organizaciones terroristas, narcotraficantes, traficantes de armas y de animales exóticos, sicarios, vendedores de información (estatal o corporativa) robada y de distintos tipos de documentos (certificados de nacimiento, licencias de conducir o pasaportes), pedófilos y también por aquellos que buscan lavar activos provenientes de actividades ilícitas.

Por otro lado, la red oscura también es útil y sirve, por ejemplo, cuando una persona debe comunicarse ocultando su identidad porque, por motivos políticos, religiosos o laborales, es víctima de persecuciones políticas, de acoso o de amenazas que pueden poner en riesgo su libertad o su vida. Retomando el propósito de la sección, téngase en cuenta, finalmente, que, según la literatura de referencia, en los diferentes planos de la *web* funcionan distintos tipos de mercados de drogas ilícitas que cuentan, cada uno, con sus propias características; en particular, puede precisarse que, en lo referido a las plataformas de comercialización de sustancias prohibidas en el plano superficial de la *web*, sobresalen, por un lado, las farmacias *on line* y, por otro, las redes sociales y los foros (Mounteney *et al.* 2016, 15-16); y que, en lo que respecta a los mercados de venta de estupefacientes en la *web* oscura, se destacan, esencialmente, los criptomercados (Mounteney *et al.* 2016, 14; Aldridge y Decary-Hétu 2016, 23).

Criptomercados

Tal como se señalara, en lo concerniente a los mercados de drogas ilícitas que operan en la *Dark Web*, puede indicarse que, en ese plano de la red, se destacan los *criptomercados* (también denominados, por algunos autores, como *mercados de red oscura*). Las principales características de este tipo de mercados virtuales son las siguientes: a) son plataformas de compra venta de productos (en su mayoría, ilegales) en línea que funcionan en la *web* oscura; b) permiten a los usuarios buscar y comparar productos y vendedores; c) tienen, desde el punto de vista estructural y funcional, un aspecto muy similar a los mercados *on line* legales que funcionan en la *web* superficial (Amazon.com o MercadoLibre.com); d) emplean un abanico de estrategias y tecnologías para ocultar la identidad de sus participantes, para lograr que las transacciones sean anónimas y para esconder la ubicación física de los servidores (Aldridge y Decary-Hétu 2016, 23). En la presente sección, que se dividirá en seis partes, se buscará presentar los principales rasgos, potencialidades, límites y desafíos que plantean los criptomercados; a la vez, se hará referencia a las estrategias que, hasta el momento, se concibieron para desmantelarlos.

Tecnologías de seguridad y mecanismos para generar confianza en consumidores y compradores

En relación con este tema, se considera apropiado distinguir aquellas tecnologías de seguridad que son requisitos indispensables para acceder y, así, poder operar en los criptomercados de aquellas que no son de uso obligatorio para ingresar a ellos, pero que, en su marco, suele recomendarse y estimularse su utilización. A su vez, también se hará referencia, finalmente, a una serie de estrategias impulsadas por los mercados de red oscura para para estimular la confianza de los usuarios en ellos.

En relación con el primer tipo de tecnologías, se debe hacer referencia a los protocolos de anonimización y a las criptomonedas. En primer lugar, se señala que, para hablar de los primeros, es decir, de los protocolos, sistemas o redes de anonimización, la exposición se centrará –sin desconocer que existen otros tales como *Invisible Internet Project* (I2P) o JAP (JonDonym15 o Java Anon Proxy)– en la *red Tor* (*The Onion Router*). El navegador *Tor* se desarrolló en el marco del Proyecto *Tor*, que, tal como lo indica Lewman (2016), es una iniciativa que se ocupa de investigar y desarrollar *software* que permita a las personas mantenerse anónimas y resguardar su privacidad en Internet. En relación con esto, puede señalarse que, entre otros productos ofrecidos en *torproject.com*, se destacan, por ejemplo: el *Tails* (*The Amnesic Incognito Live System*), que es un sistema operativo diseñado para preservar la identidad y la privacidad de los usuarios; o el *Tor Messenger*, que es un sistema de mensajería multiplataforma que envía todo su tráfico a través de la red *Tor*.

El navegador *Tor* –tal vez, el producto más conocido entre los que fueron elaborados en el seno del referido proyecto– es un *software* libre que tiene una interface similar a las de los navegadores más populares –Explorer, Chrome, Firefox, etc.–, pero que, a diferencia de ellos, permite mantener el anonimato *online* a través del ocultamiento de la dirección IP de la computadora (o del dispositivo a través del que se realice la conexión a Internet) (EMCDDA 2016, 136). Esto es así ya que, a través del aludido navegador *Tor*, se puede acceder a la red *Tor*, que cuenta con más de 7000 nodos operados por voluntarios a lo largo de todo el mundo y en el marco de la cual se trabaja con un protocolo conocido como encaminamiento o enrutamiento cebolla (Lewman 2016, 33).

En términos generales, el enrutamiento cebolla consiste en la envoltura de las comunicaciones en capas de encriptación y en su enrutamiento a nivel global (Lewman 2016, 33); de tal modo, se logra generar un entorno de interacción en Internet en el que las personas (obviamente, las que acceden a él) gozan de altos niveles de privacidad y seguridad. Como consecuencia de lo indicado, es decir, de la lógica de su funcionamiento, el navegador y la red *Tor* permiten evitar –o, por lo menos, dificultan significativamente– , por un lado, el espionaje, que se define como "la habilidad de uno o más de un actor que, de manera secreta, graba o escucha las comunicaciones de quienes están en contacto con o sin el conocimiento de ellos"; y, por otro lado, el análisis de tráfico, que es una técnica utilizada para "inferir quién está hablando con quién a través de una red pública", "cuánto hablan y con qué frecuencia se comunican" e "identificar y monitorear comportamientos e intereses" (Lewman 2016, 33).

En segundo lugar, las criptomonedas son monedas descentralizadas, es decir, no depen-

den de un cuerpo centralizado soberano de emisión para operar sino que funcionan mediante una red de pares (o red peer-to-peer) (Kruithof *et al.* 2016, xxxiii). Los usuarios son quienes dan valor a las criptomonedas; a su vez, también debe destacarse que las operaciones son distribuidas utilizando *software* de fuente abierta que puede ser utilizado en cualquier computadora o dispositivo móvil. Al ser un bien virtual –en contraposición a las unidades impresas de dinero fiduciario–, las criptomonedas no pueden ser destruidas o perdidas completamente y, a la vez, unidades nuevas son imposibles de crear (más allá del límite que se pueda alcanzar minando) (Kruithof *et al.* 2016, xxxiii).

Entre todas las criptomonedas que existen y que se utilizan en los criptomercados, el *bitcoin* es, sin dudas, la más conocida o popular (Kruithof 2016, xxxiii). Las criptomonedas, cuando se usan con precaución y adecuadamente, pueden garantizar que las transacciones en línea se lleven a cabo con un alto nivel de anonimato (Cox 2016a, 41). Entre las prácticas que se pueden adoptar para lograr mayores niveles de preservación de identidad a la hora de realizar compras con este tipo de monedas virtuales, se encuentran, por un lado, las estrategias de compra anónima de criptomonedas y, por otro lado, los mecanismos para disociar las transacciones que, con ellas, se realizan de la identidad/del comprador. En relación con estos últimos, existen algunos que son ofrecidos por los propios mercados de red oscura y otros a los que, ya sea porque el criptomercado en el que operan no brinda este servicio o porque quieren hacer aún más segura sus compras, pueden recurrir los usuarios por su cuenta (Bitcoin Fog, CoinJoin o DarkWallet) (Cox 2016a, 42-44).

En tercer lugar, existen dos estrategias que, en contraposición con lo que sucedía con los protocolos de anonimización y las criptomonedas, no configuran requisitos obligatorios para operar en criptomercados, pero que, en el marco de tales plataformas virtuales de compraventa de productos (mayoritariamente) ilícitos, sí suele recomendarse e incentivarse su utilización. Por un lado, la encriptación de mensajes, que sirve para ocultar el contenido de un mensaje de modo tal que solo pueda leerlo el destinatario deseado; entre los programas de encriptación de mensajes, se destacan, entre otros, el PGP (Pretty Good Privacy), el GPG (GnuPG) y el OTR (Off-the-Record) (Cox 2016a, 44-46). Por otro lado, la encriptación de discos duros a través de la que se trata de evitar que alguien con acceso físico a la computadora pueda llegar a ciertos archivos o a la totalidad del contenido existente en tal dispositivo (por ejemplo, el caso de los peritos de las fuerzas de seguridad que tratan de investigar el contenido de una computadora secuestrada en el marco de un allanamiento dispuesto por la justicia) (Cox 2016a, 46).

En cuarto lugar, adoptan una serie de mecanismos diseñados para minimizar las estafas y, por ende, estimular la confianza de los usuarios en los criptomercados. Primero, sistemas de reputación que, del mismo modo que los existentes en los mercados de Internet superficial que comercializan productos legales (Mercadolibre.com o Amazon.com), permiten a los usuarios de los criptomercados tener una idea de la reputación de los compradores, de sus respectivos historiales de venta y también del nivel de satisfacción que alcanzaron los usuarios que, en el pasado, les compraron (Cox 2016b, 49). Entre estos sistemas, se destacan las calificaciones y los *feedbacks*, que suelen funcionar dentro del criptomercado

y habilitarse luego de realizada la compra, y también las reseñas, que, en general, se realizan en foros que existen dentro de los mercados de la web oscura o en otras redes sociales (Cox 2016b, 49). Segundo, sistemas de pago diferido (a través de mecanismos tales como el *escrow* y, más actualmente, el *mutli signature escrow*), que consiste, a grandes rasgos, en el hecho de que el criptomercado sólo libera el pago al vendedor del producto en cuestión una vez que el comprador lo recibe y manifiesta su satisfacción con el mismo (Aldridge y Décary-Hétu 2016, 25).

La expansión de los criptomercado: límites y promesas

En relación con los factores que pueden obstaculizar el crecimiento de los criptomercados y, por ende, el incremento de su participación y relevancia en el marco del mercado global de las drogas ilícitas, resulta posible distinguir cuatro. Primero, superar la falta de confianza que han generado, por un lado, las estafas que sufrieron usuarios de estos tipos de mercados por parte de administradores o hackers que les robaron sus criptomonedas; y, por otro, los procedimientos realizados por las fuerzas de seguridad que terminaron con el cierre de muchos criptomercados (Aldridge y Decary-Hétu 2016, 26). Segundo, el hecho de poder acceder a los criptomercados supone que los usuarios tengan un nivel de conocimientos técnicos relativamente alto y que, por lo tanto, no muchas personas manejan (Aldridge y Decary-Hétu 2016, 26). En este sentido, recuérdese que, para poder operar en este tipo de mercados, resulta necesario saber usar, por ejemplo, el navegador *Tor* y las *criptomonedas*; y también que es recomendable, al mismo tiempo, manejar aplicaciones tales como, por ejemplo, el citado *Tails* y también sistemas de encriptación de mensajes.

Tercero, las compras en los criptomercados tienen una recepción diferida y, por lo tanto, no son útiles para aquellos que sienten el deseo o tienen la necesidad de consumir inmediatamente (Aldridge y Decary-Hétu 2016, 26); así, debe tenerse en cuenta que los estupefacientes que se compran un determinado día en este tipo de mercados sólo se reciben luego de pasado un determinado lapso de tiempo que varía , entre otras cosas, según la distancia que separe al comprador del vendedor y al sistema de envío postal o de encomienda que se acuerde. Cuarto, el hecho de que las compras que se realizan en los criptomercados se distribuyan a través de envíos postales o encomiendas puede hacer, que tanto compradores como vendedores, se sientan desalentados a utilizar este tipo de mercados. Esto es así porque, en la medida en que existe la posibilidad de que los envíos sean monitoreados o interceptados y en que, en muchos casos, tengan como destino final domicilios que puedan relacionarse con ellos, los consumidores –pero también los vendedores– pueden sentir –y más aún en los casos de envíos internacionales– que, al recurrir a compras que involucran los referidos mecanismos de distribución, corren más riesgos que al realizar una transacción tradicional con un *dealer* que ya conocen (Aldridge y Decary-Hétu 2016, 26).

Factores que pueden favorecer crecimiento de los criptomercados

En relación con los factores que pueden favorecer el crecimiento de los criptomercados, pueden destacarse, desde la perspectiva de los

consumidores, dos y, desde la óptica de los traficantes de drogas, también dos. Desde el punto de vista de los consumidores, se destaca, primero, la facilidad de acceso –siempre y cuando se tengan, como ya se apuntó, los conocimientos técnicos necesarios para operar en criptomercados– a un amplio abanico de variados estupefacientes de buena calidad; y, segundo, la sensación de mayor seguridad derivada del hecho de que las transacciones se realizan en un plano virtual que, además, permite –si se utilizan apropiadamente los mecanismo de seguridad indicados previamente– preservar la identidad (Aldridge y Decary-Hétu 2016, 26). Desde la perspectiva de los narcotraficantes, se pueden apuntar, primero, la sensación que, operando adecuadamente, es decir, utilizando con pericia los distintos sistemas de seguridad indicados más arriba, se reducen las posibilidades de ser arrestados; y, segundo, la posibilidad de acceder a un mercado de consumidores mucho más amplio (y, en última instancia, de carácter global) (Aldridge y Decary-Hétu 2016, 26).

El impacto de los criptomercados en los diferentes niveles del narcotráfico

En este punto, es importante empezar señalando que, a pesar del atractivo que tiene por su carácter novedoso e inclusive disruptivo, la comercialización de estupefacientes a través de la *web* y, en particular, a través de los criptomercados no ha supuesto –por lo menos, no hasta el momento– cambios a gran escala en la dinámica general del tráfico ilícito de drogas a nivel global (Von Slobbe 2016, 78). Partiendo de tal supuesto, se considera apropiado analizar, con más detalle y teniendo en cuenta lo que, por lo menos, ha sucedió hasta el momento, cómo ha impactado (o no lo ha hecho) la emergencia de los criptomercados en los diferentes eslabones o niveles del negocio del narcotráfico; específicamente, se harán seis observaciones sobre este tema.

Primero, estos nuevos mercados no han supuesto grandes cambios en el plano de la producción ni en el de la fabricación de estupefacientes: la producción de hoja de coca y la fabricación de cocaína siguen haciéndose, casi en su totalidad, en Colombia, Perú y Bolivia. Lo mismo sucede con el caso de los opiáceos, que no han dejado de elaborarse, en mayor medida, en Afganistán ni con el de la marihuana, que, en lo concerniente al continente americano, continúa produciéndose –por lo menos, a gran escala– en países tales como, por ejemplo, Paraguay o México. Segundo, tampoco su existencia ha implicado que, a la hora de abastecerse comprando grandes cargas de estupefacientes, las organizaciones criminales dejaran de hacerlo a través de contactos personales y transacciones perfeccionadas cara a cara por representantes de las bandas criminales vendedora y compradora (Von Slobbe 2016, 78); lo que sí se verifica, en este caso, es que, a la hora de establecer comunicaciones entre ellas, las organizaciones criminales utilizan sistemas y mecanismos de encriptación (Von Slobbe 2016, 78).

Tercero, a su vez, la emergencia de criptomercados no ha supuesto grandes cambios en el plano del transporte y de los envíos de cargas al por mayor; estos continúan haciéndose a través de transportes terrestres, embarcaciones, vuelos o encomiendas. Sin embargo, sí se ha verificado, en ciertos lugares, el crecimiento de la vía postal como medio de envío de estupefacientes –orientados en mayor medida a consumidores, pero también a traficantes para su abastecimiento y posterior venta– derivado

del incremento de las compras realizadas a través de mercados de la red oscura (Von Slobbe 2016, 78; Aldridge y Décary-Hétu 2016, 25).

Cuarto y relacionado con lo señalado previamente, sí puede afirmarse que los criptomercados han tenido un cierto impacto en el nivel de los intermediarios, quienes, según pudo determinarse a través de investigaciones, ven a los criptomercados como fuentes de abastecimiento de cantidades importantes de estupefacientes que, en un momento posterior, revenden (ya sea en los mismos mercados de la red oscura y/o en los mercados tradicionales) (Von Slobbe 2016, 78; Aldridge y Décary-Hétu 2016, 25). Quinto, el surgimiento de criptomercados sí ha generado cambios al nivel de la venta al por menor de estupefacientes; en este plano es, sin dudas y hasta el momento, en el que mayor impacto han tenido este tipo de nuevos mercados virtuales ya que se han erigido como una alternativa a los mercados de venta al por menor tradicionales o físicos.

En relación con esto, puede precisarse que las ventas al por menor realizadas en los criptomercados son, a diferencia de las que tienen lugar en los mercados tradicionales, anónimas y virtuales (es decir, sin contacto cara a cara entre las partes en ningún momento de la transacción); y, por ende, no acarrean el riesgo de sufrir –por lo menos, en sus formas tradicionales– violencia (física), robos (físicos) o extorsiones (Von Slobbe 2016, 78).[5] Así, en los mercados de *web* oscura, el consumidor compra *online* y abona con criptomonedas. Luego de recibir la orden de compra, el vendedor despacha el pedido a través de la vía postal. Posteriormente, el comprador lo recibe en su casa o lo retira por el domicilio que haya brindado al despachante del producto; tal como se explicó de manera previa, en muchos casos, el vendedor solo recibe el pago luego de que el consumidor haya confirmado la recepción de lo acordado.

Por último, y teniendo en cuenta que, hasta el momento, el surgimiento de los criptomercados tuvo impacto (menos significativo) en el eslabón de intermediarios (compradores al por mayor) y (más importante) en el de la venta al por menor, resulta apropiado señalar que existen dos posturas en relación con el modo en que, siempre y cuando logren aumentar en cantidad, tiempo de vida y participación en el mercado global, afectarán los criptomercados a los citados eslabones de la cadena del narcotráfico. Por un lado, se considera que, al permitir el establecimiento de vínculos directos entre productores/fabricantes y consumidores, los mercados de Internet oscura irán excluyendo del mercado a los eslabones del medio de la cadena (por ejemplo, compradores al por mayor que luego revendían a quienes comercializaban al menudeo) (Christin 2013; Martin 2013). Por otro, se afirma, a partir de investigaciones realizadas sobre el tipo de compras que se realizaron en *Silk Road*, que los criptomercados pueden, de hecho, funcionar como plataformas que faciliten el trabajo de los compradores al por mayor (Aldridge y Decary-Hétu 2014).

En un trabajo titulado *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*, Aldridge y Decary-Hétu (2014) demuestran que, en contraposición a lo que sostenían Martin (2013) o Christin (2013), *Silk Road* no era (o, por lo menos, no solo) un *Ebay para drogas*, es decir, una plataforma en la que solo se hacían

5 Sin embargo, la violencia se expresa, en los criptomercados, de modos novedosos; por ejemplo: las amenazas, las calificaciones negativas injustificadas, el *doxing* (que consiste en averiguar la identidad de un usuario a través de técnicas de hackeo para, luego, extorsionarlo), el robo, el fraude y el *cyber-bullying* (Aldridge y Decary-Hétu 2016, 28).

compras pequeñas para abastecer el consumo personal sino que, además, configuraba una mercado en el que intermediarios realizaban compras significativas para abastecerse y, luego, comercializarlas, ya sea en las calles o en criptomercados. En este sentido, los autores calculan que entre el 31% y el 45% de los ingresos de Silk Road resultaron de este tipo de transacciones (Aldridge y Decary-Hétu 2014, 12).[6] En definitiva, ambas posturas no son, desde ningún punto de vista, excluyentes. Es decir, es probable que, de manera simultánea, los mercados de la red oscura permitan la vinculación directa entre productores/fabricantes y usuarios; y también, la realización de compras al por mayor por parte de traficantes que ocupan un lugar intermedio en negocio del narcotráfico y que, posteriormente, revenderán tales estupefacientes en mercados tangibles o virtuales.

Transacciones en criptomercados: ¿cuánto, qué y entre quienes?

A partir del análisis de la literatura de referencia,[7] resulta posible agrupar en seis ejes algunas de las reflexiones que, en tal bibliografía, se realiza sobre, entre otras cosas, el volumen de las transacciones y del dinero que generan los criptomercados, el tipo de drogas que, en ellos, se compran y también el perfil de los vendedores y compradores que operan en estos mercados virtuales. En primer lugar, se señala que, desde el desmantelamiento de *Silk Road* en octubre de 2013, se triplicaron las compras de estupefacientes en criptomercados y se duplicaron las ganancias generadas por tal tipo de transacciones. Esto se ha dado a pesar de que, desde la caída del referido mercado de red oscura, se sucedieron numerosos procedimientos realizados por las fuerzas policiales que tuvieron éxito en desmantelar otros criptomercados (Kuithof *et al.* 2016, xxvi). En segundo lugar, se indica que el total de las ganancias generadas mensualmente por la venta de drogas ilícitas en criptomercados oscila, en la estimación más baja, entre 12 y los 14 millones de dólares y, en la estimación más alta, entre 21 y 25 millones de dólares (Kruithof *et al.* 2016, xxv).

Si se tiene en cuenta que, según el *Informe sobre los mercados de drogas en la UE* del Observatorio Europeo de las Drogas y las Toxicomanías (EMCDDA), el mercado (minorista) europeo de drogas ilegales produce, como mínimo, cerca de 2.000 millones de dólares al mes y, como máximo, más de 2.500 millones de dólares mensuales. Queda expuesto con claridad lo que se adelantara más arriba, es decir, que el volumen de dinero ilícito generado en los mercados de la *web* oscura es, en relación con el producido en los mercados ilegales tradicionales, físicos u *offline*, muy pequeño todavía (EMCDDA 2016, 7). En tercer lugar, se establece, por un lado, que las compras al por menor (menores a 100 dólares) representan la mayor proporción de las operaciones que se hacen en los mercados de la red oscura; y, por otro lado, que las compras al por mayor son un porcentaje pequeño del total de las transacciones que se realizan en los criptomer-

6 Lo que debe tenerse en cuenta –y, en cierta medida, los autores lo reconocen– es el hecho de que –por lo menos, no necesariamente– todas las compras al por mayor realizadas en criptomercados deban estar destinadas, posteriormente, a ser revendidas al por menor. Así, un usuario compra significativas cantidades porque: a. centraliza la compra de un grupo personas; b. puede obtener descuentos; c. cree que es más seguro recibir una vez mucho que muchas veces poco.

7 En particular del trabajo colectivo titulado *Internet facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands* y de una serie de estudios que enfocan su atención en el análisis de *Silk Road.*

cados, pero que, a pesar de eso, representan una gran proporción de las ganancias producidas en dichos mercados virtuales (alrededor del 25%) (Kruithof *et al.* 2016, xxv).

En cuarto lugar, se señala que la marihuana es el estupefaciente que más ganancias genera en los criptomercados (31%) y que lo siguen, con un 24%, los estimulantes (entre los que se incluyen la cocaína y las anfetaminas); con un 16%, las sustancias tipo éxtasis; con un 8%, los psicodélicos y, con un 6%, los opioides (Kruithof *et al.* 2016, xxv; Aldrigdge y Décary-Hétu 2014; Barrat *et al.* 2014). En este caso, si se tiene en cuenta el referido informe del EMCDDA sobre los mercados de drogas ilícitas en la UE, puede apreciarse que, en ambos tipos de mercados, el cannabis y la cocaína tienen una participación similar en el total de las ganancias mientas que el éxtasis genera más dinero en los criptomercados y la heroína, en los mercados tradicionales (EMCDDA 2016, 13).

En relación con esto, se concluye, además que, en los criptomercados, la demanda suele estar más dirigida a estupefacientes habitualmente relacionados con el consumo recreativo o con su uso en fiestas que a las llamadas drogas ilícitas duras (Kruithof *et al.* 2016, xxv; Ormby 2016, 63; Aldridge y Décary-Hetu 2014). Esto tiene que ver, en gran medida, con el hecho de que aquellas personas que, lamentablemente, sufren una adicción a dichas sustancias no están en condiciones de manejar la demora que existe entre el momento en que compran *on line* el estupefaciente en cuestión y el momento en que lo reciben (Ormby 2016, 63). En quinto lugar, se indica la mayoría de los vendedores que operan en los criptomercados son de Estados Unidos, Australia, Canadá y Europa Occidental. En particular, los vendedores de mercados de la *web* oscura actúan en Estados Unidos son los que manejan la mayor cuota de mercado (35,9%); luego, se ubican los que operan en Gran Bretaña (16,1%), en Australia (10,6%), en Alemania (8,4%) y en Holanda 7,1% (Kruithof *et al.* 2016, xxvii).

En sexto lugar, se establece que, si bien todavía no hay suficiente evidencia para alcanzar conclusiones sólidas, tanto los compradores como los vendedores que operan en criptomercados suelen ser hombres jóvenes (menores de 40 años) de países angloparlantes o ubicados en Europa Occidental; que tienen buenos niveles educativos, carácter emprendedor y altas habilidades tecnológicas (Kruithof *et al.* 2016, xxix). A su vez, se precisa que, entre los vendedores, se observa una combinación entre novatos o principiantes y profesionales con experiencia previa en mercados tradicionales que consideran a los criptomercados como una nueva y adicional vía para generar ingresos (Kruithof *et al.* 2016, xxix; Ormsby 2016, 62-63). Al mismo tiempo, se advierte que muchos vendedores trabajaban solos mientras que otros, los que manejan mayores volúmenes de ventas, forman equipos para poder satisfacer todas las demandas que reciben (Ormsby 2016, 63).

También se indica que la mayoría de los que compran estupefacientes en criptomercados son personas que, en el pasado, ya consumieron estupefacientes y que suelen usarlos recreativamente (Ormsby 2016, 62). Además, compran en estos mercados virtuales porque les ofrecen más seguridad (no exposición a formas tradicionales de violencia), alta disponibilidad, gran variedad, buena calidad y facilidades y velocidad de entrega (Ormsby 2016, 64; Kruithof *et al.* 2016, xxix). A su vez, al hablar de los compradores, también puede señalarse que una proporción no menor de ellos

suelen defender o hacer propios –con diferentes niveles de apegos– ciertas ideas o postulados libertarias (Ormsby 2016, 62).

Silk Road y criptomercados: características, tendencias e interrogantes

Silk Road fue un criptomercado que funcionó desde febrero 2011 hasta octubre de 2013, mes en el que fue desmantelado por el FBI (*Federal Bureau of Investigation*), y que estaba dedicado, casi exclusivamente, a la venta de estupefacientes. Del mismo modo que el resto de los mercados de este tipo, esta plataforma *on line* de compraventa de productos (en su mayoría) ilícitos tenía un aspecto visual y una lógica funcional muy parecidas a, por ejemplo, las de Ebay.com, es decir, a las de otros mercados legítimos que funcionan en el plano superficial de la *web* (Aldridge y Decary-Hétu 2016, 24). En *Silk Road*, los usuarios buceaban por el sitio para buscar los productos que deseaban y, en el proceso, tenían la posibilidad de comparar precios y reputaciones de vendedores a partir de las calificaciones y los comentarios realizados por otros consumidores. Una vez que el usuario decidía lo que quería comprar, ordenaba el producto y lo pagaba con criptomonedas. Lo interesante de *Silk Road* es que, utilizando el mecanismo de pago diferido descrito previamente, protegía a quien realizaba la compra ya que solo permitía que el vendedor recibiera el dinero abonado por el comprador luego de que éste manifestara su satisfacción con la recepción del producto que había pagado (Aldridge y Decary-Hétu 2016, 24).

Según las estimaciones disponibles, pudo determinarse que, a lo largo de su existencia, *Silk Road* generó más de 1.200 millones de dólares en ventas, que involucraron alrededor de 150.000 compradores y 4.000 vendedores (Sui *et. al.*, 2015: 5). A su vez, también puede destacarse, para tomar conciencia de lo rentable que fue este negocio ilícito, que, al ser detenido Ross Ulbritch, se le incautaron 174.000 bitcoins; tal cantidad de criptomonedas equivalen a 159.906.000 millones de dólares (si se tiene en cuenta el valor que tuvo el bitcoin el 27 de enero de 2017). *Silk Road* se convirtió, sin dudas, en el criptomercado más famoso: ha tenido –y sigue teniendo– una gran presencia en los medios masivos de comunicación, cuenta con innumerables referencias en los trabajos académicos sobre la materia y también ha sido el tema central de audiovisuales tales como, por ejemplo, el documental *Deep Web*, que fue estrenado en 2015.

Sin embargo, el hecho de que *Silk Road* se haya convertido en el criptomercado más conocido no supone, bajo ningún concepto, que haya sido el único ni el más grande; entre otros, resulta posible destacar los siguientes: Sheep, Pandora, Agora, Hydra, Evolution, Silk Road 2.0, Cloud 9 (Aldridge y Decary-Hétu 2016, 24). El volumen de ganancias generadas por *Silk Road*, la dinámica de su funcionamiento, su corta duración –rasgo que comparte con el resto de los criptomercados a los que se hizo referencia en el párrafo previo– y los conocimientos técnicos necesarios para construirlo y operar en él permiten, siguiendo a la literatura especializada, realizar una serie de observaciones sobre tendencias o rasgos que comparten y también sobre interrogantes que plantean los mercados que operan en la red oscura.

Primero, los criptomercados son plataformas que, para funcionar, implican la participación de numerosos actores; en particular, puede distinguirse dos tipos. Por un lado, los

actores clave o fundamentales, que son los administradores, los desarrolladores, los moderadores, los vendedores y los compradores. Por otro lado, otros actores que, a priori, no suelen ser considerados, pero que, ya sea voluntaria o involuntariamente, están involucrados en el funcionamiento de este tipo de mercados; entre ellos, se destacan, por ejemplo, los proveedores de servicios de Internet, los empresas que ofrecen servicios postales y los operadores de criptomonedas (Van Slobbe 2016, 79; Kruithof *et al.* 2016, xxix).

Segundo, la mayoría de los criptomercados suele tener una existencia corta; a su vez, puede añadirse que sus respectivos cierres derivan más de estafas (básicamente, el administrador del sitio o alguien que identifica y explota una falla en el sistema de seguridad de la plataforma roba las criptomonedas que pertenecen a los usuarios del mismo) que de la intervención de las fuerzas policiales (Aldridge y Decary-Hétu 2016, 24). Tercero, si bien es cierto que, en ellos, se realizan numerosas transacciones y que estas generan importantes sumas de dinero, también es verdad que las ventas que se efectúan en estos mercados y las ganancias que estas generan no representan –por lo menos, hasta el momento y tal como ya se apuntó– más que una porción mínima de las transacciones y dinero producido por el mercado global de drogas ilícitas (Aldridge y Decary-Hétu 2016, 25).

En algún punto, resulta lógico que así sea porque, hasta el momento y como ya se expuso previamente, la mayor parte del abastecimiento, del tráfico, de la distribución y de la comercialización (tanto al por mayor como al por menor) todavía descansan en redes de productores, distribuidores, macrotraficantes, vendedores y consumidores que operan, esencialmente, en el mundo físico y en los mercados tangibles (Martin 2014; Aldridge y Decary-Hétu 2016, 25). Cuarto, puede señalarse, en relación con las aptitudes necesarias para triunfar en los criptomercados, que ya no es importante, como sí lo era en el caso de los mercados tradicionales, el nivel de control territorial, el poder de fuego o el grado de penetración de actores estatales alcanzado por una organización delictiva; sino que, en el marco de estos mercados de la *web* oscura, resulta decisivo, para los criminales, contar con conocimientos técnicos (aquellos que no sólo permiten operar en ellos sino que, además, posibiliten hacerlo del modo más seguro posible), con conocimientos de marketing *on line* (armar un perfil adecuado en el mercado que elija para vender) y con una buena reputación basada en el cumplimiento de las transacciones y en la oferta de productos de calidad (Aldridge y Decary-Hétu 2016, 27-28).

Quinto –y solo como un ejercicio preliminar y, tal vez, apresurado–, se considera que, a partir de analizar el caso de *Silk Road* y la biografía de su creador, Ross Ulbricht (dos títulos, un grado en física gracias a una beca completa y una maestría en ingeniería, varios años dedicado a la investigación científica, numerosas publicaciones en revistas científicas y fundación de emprendimientos legales tales como *Good Wagon Books*, una plataforma para la venta de libros con un enfoque solidario), puede resultar apropiado, por lo menos, plantearse la posibilidad de preguntarse y pensar en si la existencia de criptomercados no supone, a la vez y en algunos casos, la emergencia, en los algunos niveles de la cadena de este negocio ilícito, de un nuevo e inédito perfil de narcotraficantes. Finalmente, a pesar de que existen algunos estudios y especulaciones sobre el tema, también resultaría interesante, teniendo en cuenta todo lo expuesto, emprender líneas

de investigación que se planteen analizar, en profundidad, cómo ha impactado la emergencia de los criptomercados en la anatomía y estructura de las organizaciones criminales dedicadas al narcotráfico (y en especial, a las que operan en los eslabones intermedios y de venta al por menor).

Estrategias para luchar contra el narcotráfico en los criptomercados

En relación con las estrategias que, hasta el momento, han impulsado las fuerzas policiales para luchar contra el tráfico ilícito de estupefacientes en la red oscura, pueden distinguirse, siguiendo a Kruithof *et. al.*, cuatro: técnicas tradicionales de investigación que se aplican, también, en los mercados físicos (por ejemplo, vigilancia o, en el caso de que las legislaciones nacionales las permitan, operaciones encubiertas); identificación e intercepción de envíos postales o encomiendas; la detección *on line* (rastreo de flujos de dinero, monitoreo de mercados de Internet oscura, uso de técnicas de *big data*); y el desmantelamiento de grandes criptomercados (Kruithof *et al.* 2016, xxx). En vinculación con este último punto, que es, en gran medida, el que ha concentrado buena parte del interés de las fuerzas policiales, puede señalarse que, en simultáneo con el quiebre de un criptomercado y siempre en relación con él, se intenta incautar grandes volúmenes de estupefacientes, incautar la mayor cantidad posible de bienes que fueron obtenidos ilícitamente por los delincuentes (especialmente, criptomonedas); y, además, detener para, posteriormente, enjuiciar a sus administradores y moderadores y también a quienes, en su marco, se hubieran convertido en grandes vendedores (Von Slobbe 2016, 80).

Al impulsar las estrategias indicadas (especialmente, la que se hizo referencia en el párrafo previo) las fuerzas de seguridad buscan que los usuarios pierdan confianza en la plataforma, es decir, intentan quebrar "el aura de anonimidad y la sensación de ser intocable que se asocia con ella" (Von Slobbe 2016, 81). En relación con la profundidad y la extensión del impacto que, hasta el momento, han tenido este tipo de estrategia en el tráfico ilícito de estupefacientes que se realiza en la *web* oscura, todavía no existe, según la literatura de referencia, información suficiente para establecer tendencias o conclusiones definitivas. Sin embargo, sí pueden realizarse, sobre este tema, dos observaciones preliminares: primero, que, luego del desmantelamiento de un gran criptomercado, suelen surgir, rápidamente, otros que lo reemplazan; y, segundo, que, en términos de medidas de seguridad, estos nuevos criptomercados se caracterizan por haber aprendido y evolucionado, es decir, por haber analizado qué llevó a la caída a sus antecesores y por haber buscado soluciones para esas debilidades (Von Slobbe 2016, 81).

En vinculación con este último punto, es decir, con la resiliencia de los mercados de la web oscura, debe destacarse una tendencia que se está observando y que, de consolidarse, se convertiría en un significativo obstáculo para las fuerzas policiales en su lucha contra el tráfico ilícito de estupefacientes en Internet. En particular, se hace referencia al hecho de que han ido surgiendo criptomercados que, a diferencia de los conocidos hasta el momento, son descentralizados, es decir, operan usando una red P2P (*peer to peer*) y, al hacerlo, hacen que resulte realmente difícil –o casi imposible– desmantelarlos completamente (Lewman 2016, 37; Mounteney *et al.* 2016, 130; Kruithof *et al.* 2016, xxvii).

Por último, en relación con las medidas que podrían adoptarse para reforzar las estrategias que, hasta el momento, han impulsado las fuerzas policiales para combatir el narcotráfico en criptomercados, pueden destacarse las siguientes: aumentar la inversión y profundizar la utilización de técnicas de big data para intentar vincular los apodos y la actividad en la web delos vendedores con alguna dirección de IP; incrementar, ya sea incorporando nuevos y/o capacitando a los que están en actividad, los recursos humanos que cuenten con la formación técnica necesaria para luchar contra este tipo de delitos; establecer acuerdos entre el Estado y los proveedores de servicios de Internet para evitar que, aun sin ser conscientes de ello, los criptomercados funcionen en sus servidores; promover revisiones y actualizaciones del marco normativo que regula la materia; impulsar –con especial énfasis– la cooperación y la coordinación internacional; estimular los acuerdos con los operadores postales para incrementar las capacitaciones y también impulsar el aumento del uso y la actualización de la tecnología orientada a detectar los envíos de estupefacientes a través de la vía postal; elaborar campañas dirigidas a minar la confianza de vendedores y compradores en la fiabilidad de los mercados de Internet oscura (Jardine 2015, 8-11; Von Slobbe 2016, 82).

Reflexiones finales

Atento al interés y a la preocupación que, en múltiples actores, han suscitado los mercados de red oscura, el presente artículo se propuso, tomando como referencia lo expuesto por la bibliografía especializada, hacer una presentación sistemática accesible y en castellano de los principales rasgos de los criptomercados. A partir de lo trabajado, se considera que la notable atención que estos mercados virtuales han concentrado debe relacionarse más con su carácter innovador que con su impacto en la dinámica general del tráfico ilícito de drogas, que ha sido muy limitado hasta el momento. A su vez, es posible que, superada la novedad, el hecho de que sigan suscitando tanto interés dependa del modo en que evolucionen.

En relación con esto, son varios los interrogantes que se vislumbran en el horizonte de los criptomercados: ¿mantendrán su tendencia creciente o, por el contrario, se contraerán como resultado de la intervención de las fuerzas de seguridad? ¿Lograrán, en caso de expandirse, ampliar su influencia a más eslabones de este negocio criminal? ¿Cómo impactará en ellos el hecho de que, en solo unas décadas, el mercado de consumo estará formado, en mayor medida, por generaciones nacidas y criadas, enteramente, en entornos digitales? ¿Supondrá su consolidación el surgimiento de un perfil de narcotraficante desconocido hasta el momento? ¿Lograrán, de expandirse, aumentar su participación en las ganancias totales generadas por el tráfico ilícito de drogas a nivel mundial? ¿Asimilarán, para consolidarse, nuevas tecnologías tales como las que están desarrollándose en el campo de la inteligencia artificial y del *big data*?

De haber alcanzado su objetivo, este artículo aspira a configurar un modesto punto de partida para la apertura de líneas de trabajo que, entre otras cosas, permitan ir ensayando respuesta a los interrogantes planteados, posibiliten profundizar el conocimiento sobre el tema (en particular, dentro de la región) y brinden herramientas para estar mejor preparados para enfrentar este desafío. Específicamente, el trabajo anhela: a) convertirse en el puntapié inicial de una agenda de investi-

gación sobre el uso de criptomercados en el país y en otros estados de América Latina; b) llamar la atención y estimular el interés en este tema de académicos de la región dedicados a temas de seguridad (en particular, a narcotráfico), quienes, hasta el momento, no han enfocado su atención en este actual –aunque ya no tan nuevo– fenómeno; c) convertirse en una herramienta útil y accesible para introducir en el tema a actores políticos, judiciales y agentes de las fuerzas de seguridad latinoamericanos preocupados por la problemática.

Bibliografía

Aldridge, Judith, y David Decary-Hétu. 2014. "Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation". *Documento de trabajo*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643.

_____. 2016. "Cryptomarkets and the future of Illicit drug markets". En *The Internet and drug markets*, editado por EMCDDA, 23-32. Lisboa: EMCDDA.

Buxton, Julia, y Tim Binghman. 2015. "The rise and challenge of dark net drug markets". *Global Drug Policy Observatory Policy Brief* 7: 1-24. https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf.

Chertoff, Michael, y Tobby Simon. 2015. "The impact of the dark web on the Internet governance and cyber security". *Global Comission on Internet Governance Paper series* 6:1-8. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

Christin, Nicolas. 2013. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace". *Documento de trabajo*, https://arxiv.org/pdf/1207.7139.pdf.

Cox, Joseph. 2016a. "Staying in the shadows: the use of bitcoin and encryption in cryptomarkets". En *The Internet and drug markets*, editado por EMCDDA, 41-48. Lisboa: EMCDDA.

_____. 2016b. "Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets". En *The Internet and drug markets*, editado por EMCDDA, 49-56. Lisboa: EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction. 2014. *Informe europeo sobre drogas 2014. Tendencias y novedades*. Lisboa: EMCDDA.

_____. 2015. *Informe europeo sobre drogas 2015. Tendencias y novedades*. Lisboa: EMCDDA.

European Monitoring Centre for Drugs and Drug Addiction y EUROPOL. 2016. *Informe sobre los mercados de drogas en la UE. Visión de conjunto estratégica*. Luxemburgo: UE.

EUROPOL. 2013. *EU serious and organized crime threat assessment.* La Haya: EUROPOL.

_____. 2017. EU serious and organized crime threat assesment. La Haya: Europol.

Garcia Galera, María del Carmen, y Angharad Valdivia. 2014. "Prosumidores mediáticos. Cultura participativa de las audiencias y responsabilidad de los medios". *Comunicar* 43 (XXII): 10-13.

Jardine, Eric. 2015. "The Dark Web Dilemma: Tor, Anonymity and Online Policing". *Global Comission in Internet Government Paper Series* 20: 1-13. https://www.cigionline.org/sites/default/files/no.21.pdf.

Kruithof, Kristy, Judith Aldrige, David Décary-Hétu, Megan Sim, Elma Dujso y Stijn Hooners. 2016. *Internet facilitated drug trade. An analysis of the size, scope and the role of the Netherlands*. Cambridge: RAND.

Lavorgna, Anita. 2016. "How the use of the Internet is affecting drug trafficking practices". En *The Internet and drug markets*, editado por EMCDDA, 85-92. Lisboa: EMCDDA.

Lewman, Andrew. 2016. "Tor and links with cryptomarkets". En *The Internet and drug markets,* editado por EMCDDA, 33-40. Lisboa: EMCDDA.

Martin, James. 2014. *Drugs on the dark net. How cryptomarkets are transforming the global trade in Illicit drugs*. Nueva York: Macmillan.

Martin, James. 2014. "Lost on the Silk Road: Online drug distribution and the 'cryptomarket'". *Criminology and Criminal Justice* 14 (3): 351-367.

Mounteney, Jane, Alberto Oteo y Paul Griffiths. 2016. "The Internet and drug markets: shining a ligh on these complex and dynamic system". En *The Internet and drug markets,* editado por EMCDDA, 13-18. Lisboa: EMCDDA.

National Association Boards of Pharmacy. 2016. *Internet Drug Outlet Identification Program Progress Report for State and Federal Regulators: July 2016*. Ilinois: NABP.

Ormsby, Eileen. 2016. "Silk Road: insights from interviews with users and vendors". En *The Internet and drug markets*, editado por EMCDDA, 61-68. Lisboa: EMCDDA.

Rand Europe. 2016. *The role of the ´dark web´ in the trade of illicit drugs*. Cambridge: RAND.

Scamell, Lynda, y Alessandra Bo. 2016. "Online supply of medicines to illicit drug markets: situation and responses". En *The Internet and drug markets,* editado por EMCDDA, 107-114. Lisboa: EMCDDA.

Soska, Kyle, y Nicolas Christin. 2015. "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem". Ponencia presentada en el *24th USENIX Security Symposium*, Washington D.C., USENIX Association, 12-14 de agosto.

Thanki, Danica, y Brian Frederik. 2016. "Social media an drug markets". En *The Internet and drug markets,* editado por EMCDDA, 115-124. Lisboa: EMCDDA.

Van Slobbe, Joost. 2016. "The drug trade on the deep web: a law enforcement perspective". En *The Internet and drug markets*, editado por EMCDDA, 77-84. Lisboa: EMCDDA.