Enero - Junio 2026 año 13 no. 25

ISSN 2683-1481

UNIVERSIDAD DE GUADALAJARA

Diagnóstico FACIL Empresarial, Finanzas, Auditoría, Contabilidad, Impuestos, Legal

DIVISIÓN DE CONTADURÍA
CENTRO UNIVERSITARIO DE CIENCIAS
ECONÓMICO ADMINISTRATIVAS

CEHP

CIEF
CENTRO DE INVESTIGACIÓN EN ESTUDIOS FISCALES

Diagnóstico FACIL Empresarial / ISSN 2683-1481
Año 13, Núm. 25, pp. 34-44, Enero • Junio 2026
https://doi.org/10.32870/dfe.vi25.179

División de Contaduría / cucea
Universidad de Guadalajara

La fiscalización del comercio electrónico en el mercado de drogas ilícitas en línea

Monitoring E-commerce in the Online Illicit Drug Market

Fecha de recepción: 30/06/2025
Fecha de revisión: 01/07/2025

Fecha de aceptación: 23/10/2025
Fecha de publicación: 15/12/2025

Ricardo Ruíz García [Investigación]. Universidad de Guadalajara/Jalisco/México | ruizgarciajuridicofiscal@gmail.com | https://orcid.org/0000-0003-0210-7998. Juan José Serratos Cervantes [Metodología]. Universidad de Guadalajara/Jalisco/México | juanjoseserratos@hotmail.com | https://orcid.org/0009-0003-8406-545X.

Resumen

En esta investigación se diagnostica la insuficiencia del marco jurídico-fiscal y de las estrategias de seguridad de México para fiscalizar el comercio electrónico de drogas ilícitas. Se argumenta que el enfoque tradicional, centrado en la materialidad del delito, resulta contraproducente en el entorno digital, pues incentiva el desplazamiento de la oferta y la demanda hacia "mercados cerrados".

Lo anterior en redes sociales, consolidando una economía subterránea que erosiona la base gravable y opera con total invisibilidad. Por lo cual, a través de un método cualitativo, comparativo y documental, se demuestra la hipótesis de que las políticas actuales, lejos de mitigar el problema, fortalecen e incrementan estos mercados cerrados en redes sociales como lo son WhatsApp, Facebook e Instagram.

Con base en ello y en una arista comparativa, se estudian como marco de referencia las intervenciones internacionales contra criptomercados ("Operación Onymous") y los modelos de control de red de China y Rusia, no para replicarlos, sino para adaptar sus principios de gobernanza proactiva en temas actuales, en el caso de las drogas a través de una metodología de problemas perversos, además.

Se concluye que México debe abandonar la inacción y afirmar su soberanía digital. Para ello, se proponen líneas de acción: una reforma jurídica para tipificar el "narcomenudeo digital" y establecer la responsabilidad solidaria de las plataformas; la creación de una fuerza de tarea de ciberinteligencia, y el desarrollo de una política que exija el cumplimiento de la ley mexicana a las empresas tecnológicas.

Palabras clave: fiscalización, comercio electrónico, mercados ilícitos en línea, economía subterránea, ciberseguridad.

Abstract

This research diagnoses the inadequacy of Mexico's legal and fiscal framework and security strategies to control the e-commerce of illicit drugs. It argues that the traditional approach, centered on the materiality of the crime, is counterproductive in the digital environment, as it encourages the displacement of supply and demand toward "closed markets".

This is happening on social media, consolidating an underground economy that erodes the tax base and operates completely invisible. Therefore, through a qualitative, comparative, and documentary method, the hypothesis is demonstrated that current policies, far from mitigating the problem, actually strengthen and increase these closed markets on social media such as WhatsApp, Facebook, and Instagram.

Based on this and from a comparative perspective, the international interventions against crypto markets ("Operation Onymous") and the network control models of China and Russia are studied as a frame of reference, not to replicate them, but to adapt their principles of proactive governance to current issues, in the case of drugs through a wicked problem methodology.

The conclusion is that Mexico must abandon inaction and assert its digital sovereignty. To this end, the following lines of action are proposed: a legal reform to criminalize "digital drug dealing" and establish joint liability for platforms; the creation of a Cyberintelligence Task Force; and the development of a policy requiring technology companies to comply with Mexican law.

Keywords: oversight, e-commerce, illicit online markets, economy.

Introducción

Nos encontramos en la era de la inteligencia artificial, la digitalización; un entorno de oportunidades y a su vez de peligros significativos. Uno de los desafíos más apremiantes para la recaudación fiscal es la desvinculación entre el lugar donde se genera valor y donde se pagan los impuestos, un fenómeno que erosiona la base gravable al estar las reglas fiscales tradicionales ancladas a la presencia física.

Las economías subterráneas en línea, como el comercio de drogas, explotan esta desconexión de manera extrema, generando transacciones dentro de una jurisdicción sin nexo físico, lo que les permite una total invisibilidad ante la autoridad hacendaria. Esta investigación se centra en el mercado de drogas ilícitas en línea dentro del contexto mexicano caracterizado por un modelo híbrido de mercado.

Dicho mercado utiliza redes sociales comunes (Facebook, Instagram, WhatsApp) y métodos de entrega físicos. Se analizan las deficiencias de las políticas del Estado mexicano para fiscalizar, regular e investigar esta modalidad de mercado a través de un marco comparativo y donde se evidencia el rezago legislativo y operativo de México ante delitos cibernéticos de "segunda generación".

El punto de partida es el diagnóstico de la ineficacia de las políticas actuales. La estrategia frontal y material contra el narcotráfico, enfocada en incautaciones y criminalización, resulta contraproducente en el entorno digital. En lugar de mitigar el problema, incentiva el desplazamiento de la oferta y la demanda hacia mercados cerrados en línea, lo cual disminuye la percepción de riesgo del consumidor.

Lo cual además fortalece una economía subterránea que evade la fiscalización y la acción de la justicia. El objetivo general es, por tanto, exponer el efecto de las estrategias actuales en el combate a los mercados ilícitos de drogas en línea y diagnosticar la insuficiencia del marco jurídico fiscal mexicano para regular y fiscalizar dicho comercio.

Problema de investigación

De acuerdo con la investigación realizada, se observa como problema central, la ineficacia y obsolescencia de las estrategias de seguridad y del marco jurídico-fiscal de México para combatir el comercio electrónico de drogas ilícitas. Esto, ante un enfoque tradicional centrado en la materialidad del delito (incautaciones y criminalización de usuarios), ignora la migración del narcotráfico al ciberespacio.

Como consecuencia, en lugar de reducir el mercado, las políticas actuales provocan su desplazamiento hacia plataformas digitales y "mercados cerrados",[1] lo que consolida una economía subterránea que opera con total invisibilidad para el Estado, lo que además de erosionar la base gravable, anula las facultades de comprobación fiscal y genera flujos de riqueza no fiscalizables.

Con base en lo anterior, y en un contexto tecnológico actual,[2] ante ello la inteligencia humana debe ser una pieza fundamental dentro de la virtualidad y sus implicaciones; como señala Tapscott (1997): "[…] La economía digital trae consigo numerosas promesas y oportunidades ilimitadas para la creación de riqueza y desarrollo social. A la vez, implica peligro potencial […]".

Por otra parte, señala la OCDE (2020) que "[…] el principal desafío de la economía digital para la recaudación fiscal es la desvinculación entre el lugar donde se genera valor y el lugar donde se pagan los impuestos […]" Este fenómeno es la base de la erosión de la base gravable, ya que las reglas fiscales tradicionales se basan en la presencia física para determinar dónde se debe pagar el impuesto.

Por ello, las economías subterráneas en línea, como el comercio de drogas en redes sociales, explotan esta misma desconexión a un nivel más extremo: generan valor y realizan transacciones dentro de la jurisdicción de un país sin tener ningún nexo físico, lo que les permite operar con total invisibilidad para la autoridad hacendaria y eludir completamente el pago de impuestos.

Es por ello que algunos de esos peligros potenciales se observan en la ilegalidad de los mercados de drogas y el comercio electrónico que se desarrolla en línea, objeto de nuestro estudio en este trabajo de investigación, y la necesidad apremiante de establecer controles educativos, administrativos, cibernéticos, económicos, jurídicos y de seguridad pública, entre otros, que representa y requiere este problema perverso.

El fenómeno del comercio de drogas ilícitas en línea dentro del contexto mexicano, como objeto de estudio, caracterizado por un modelo híbrido que utiliza redes sociales de acceso común (como Facebook, Instagram y WhatsApp) para la concertación de transacciones, combinadas con métodos de entrega físicos, será estudiado desde las deficiencias de las políticas y estrategias del Estado mexicano para fiscalizar, regular e investigar esta modalidad de mercado.

A diferencia de lo señalado en el párrafo anterior, los mercados internacionales en cuanto a criptomercados, que operan con tecnologías de anonimización y criptomo-

1 Redes sociales como Facebook, Instagram, WhatsApp.

2 Inteligencia artificial, digitalización, internet, o las tecnologías financieras, de información y comunicación.

nedas, utilizándolos como un marco de análisis comparativo, evidencia el rezago legislativo y operativo de México ante delitos cibernéticos de segunda generación como el del comercio electrónico de drogas ilícitas. Esto, sin centrarnos en una droga específica.

Por lo tanto, al no centrar el análisis de este estudio en una droga específica, se evalúa primordialmente la estructura del mercado virtual, sus canales de distribución y las implicaciones fiscales, económicas y de seguridad pública que se derivan de su existencia fuera del alcance efectivo del Estado. Con base en ello, se buscará como objetivo general exponer el efecto de las estrategias al combate de los mercados ilícitos de drogas en línea.

Es decir, diagnosticar la insuficiencia del marco jurídico fiscal mexicano para regular y fiscalizar el comercio electrónico de drogas ilícitas. Esto para buscar hallazgos respecto de la estrategia de seguridad pública, al incentivar la migración de estos mercados a plataformas digitales, lo que genera economía subterránea que erosiona la base gravable potencial y flujos de riqueza no fiscalizables.

Aunado a lo anterior, demostrar que si continuamos con un enfoque tradicional, centrado en la materialidad del delito, es contraproducente en el entorno digital; acciones que, lejos de mitigar el problema, incentivan el desplazamiento de la oferta y la demanda hacia mercados cerrados en línea, fortaleciendo una economía subterránea que evade la fiscalización y la acción de la justicia.

Por lo que de acuerdo con Tapscott (1997), lo que representaría el rezago tecnológico a los individuos o empresas y sus consecuencias; para el tema de estudio, representa no sólo un rezago sino un área de oportunidad que la delincuencia o crimen organizado han utilizado ante una urgente fiscalización del comercio electrónico de las drogas ilícitas en línea. Lo anterior, con sustento en la característica principal de los negocios virtuales que se gestan; según Sostres (2010):

> [...] su estructura organizativa se apoya en el uso de Internet para ampliar sus transacciones y operaciones en el mercado del ciberespacio. En el mundo contemporáneo está proliferando y se ha transformado en una nueva organización básica de trabajo asociado de individuos y empresas que se instalan utilizando la tecnología Internet.

Por lo tanto, nuestro punto de partida en la investigación es un diagnóstico que evidencia la ineficacia de las políticas actuales en México frente a la evolución del narcotráfico hacia el ciberespacio. Como estrategias obsoletas al bastar el combate al narcotráfico en una estrategia frontal y material, enfocada en la incautación de drogas y la criminalización de usuarios, ignorando la migración del delito a plataformas virtuales.

Asimismo, esta estrategia tradicional no reduce el mercado, sino que provoca su desplazamiento geográfico y virtual hacia "mercados cerrados" en línea, donde los participantes perciben un menor riesgo y operan fuera del alcance de las autoridades. Además de carecer de una legislación digital adecuada para enfrentar la ciberdelincuencia de "segunda generación", como los criptomercados o el narcomenudeo en redes sociales.

En la actualidad los delitos informáticos que se siguen son de "primera generación", como el fraude o robo de identidad, lo que deja un vacío legal y operativo respecto a lo señalado al repercutir en falta de una fiscalización y regulación efectiva del comercio electrónico, lo que permite la consolidación de una "próspera economía subterránea", que no sólo impacta la salud y la seguridad pública, sino lesiona la economía formal y la capacidad recaudatoria del Estado.

Con sustento en lo anterior, la presente investigación mediante un eje de fiscalización del comercio electrónico internacional orientado a dichos mercados ilícitos, buscará teorizar el aprendizaje con base en la experiencia de Estados Unidos y Europa, respecto de estos mercados cerrados como los "criptomercados", ya que dichos modelos de negocio pueden acercarnos a la economía subterránea derivada del comercio electrónico. Se observará en la investigación respecto a Estados Unidos y Europa en 2014 y como antecedente inmediato el Programa Onymous, que fue parte de las estrategias para el combate y represión de dicha actividad económica virtual, y sólo han funcionado a corto plazo ante la falta de percepción de riesgo por parte de distribuidores y consumidores, es decir, no obstante el antecedente, no ha sido tan efectivo ante la peculiaridad y desplazamiento del problema.

Sin embargo, se debe tomar en cuenta que si bien las transacciones en los mercados del narcomenudeo en México generalmente se realizan mediante transacciones bancarias previamente realizada la transacción en redes sociales, para la realidad virtual mexicana los mercados de bitcoins no son ajenos, sobre todo para monopsonios y grandes empresas del narcotráfico, que es un medio más para el trato financiero de su patrimonio.

Se reitera pues que en México los canales de distribución permean a través de grupos cerrados de Facebook, Instagram o WhatsApp, en un híbrido de negocios virtuales y negocios tradicionales con la entrega de los diversos bienes como característica de materialidad de los negocios tradicionales, pero consumando el mercado de forma cibernética lejos de esta premiosa fiscalización a los citados mercados, donde cada vez más se fortalece esta virtualidad ilícita.

Esta situación en México carece de políticas y estrategias vigentes *ad hoc* al desarrollo de esta diversidad de cana-

les para delinquir, por ende, dejando un flanco totalmente descubierto en el combate a estas conductas que lesionan la economía, el poder del Estado e irrumpen en conductas típicas aún no reguladas que se apartan de la realidad material e histórica tradicional de la guerra al crimen organizado.

En esa tesitura, las formas tradicionales de combate existentes sólo aumentan el comercio en los mercados cerrados que van en aumento, ante la percepción de un bajo riesgo por parte de los involucrados, como incluso señalan Décary *et al*.: la "próspera economía subterránea que se ve impulsada por un crecimiento dramático en el número de personas que participan en mercados ilícitos en línea y una gama cada vez mayor de bienes y servicios que están disponibles" (2017).

Por lo anterior, y sin avocarnos a una droga en específico, sino al hecho propio del mercado de drogas ilícitas en línea y sus problemas de fiscalización, regulación e investigación que esto conlleva ante la rapidez con la cual se gesta y desarrollan estos mercados, en la economía formal e incluso en esta nueva era de las empresas de tecnología financiera, representan un verdadero reto para los Estados y su política fiscal, monetaria y arancelaria.

Y por parte de las drogas ilícitas en línea, representan ya un problema en México que ha salido literalmente de esta realidad de manera preocupante como generador de un submundo de mercados cerrados, directo e inmediato ante las bondades de la red, estableciendo medularmente a comprador y vendedor en un entorno seguro y fuera del radar del Estado, por lo cual resulta pertinente y se justifica la presente investigación a desarrollar dentro de los negocios virtuales.

Tema referido dentro de la economía digital que atiende al estudio de la deficiente tendencia de fiscalización y vigilancia en la política de combate a las drogas, la cual continúa enfrentándose a la materialidad de las acciones de los grupos delictivos, dejando de lado las fuentes de financiamiento y el trabajo que se comienza a vislumbrar en materia de esta economía virtual, como nuevo canal de distribución.

Además, con la capacidad de interrumpir la venta de drogas ilícitas en los grupos de delincuencia organizada y, en consecuencia, interrumpir la capacidad de las fuerzas del orden público para regular estos mercados ilícitos, que contrario a esto, la política de combate al narcotráfico solamente ayuda a estos mercados a verse fortalecidos al momento de cambiar de un mercado abierto a mercados cerrados.

Acorde con lo anterior, la focalización de los esfuerzos establecidos en convenios internacionales en materia de economía virtual, como los establecidos por parte de importantes grupos político-económicos como el G20, a través de la Organización para la Cooperación y el Desarrollo Económico y los 15 postulados que pretenden contrarrestar la erosión de la base imponible y el desplazamiento de beneficios, sólo es un instrumento de carácter fiscal.

Por lo que desarrollar una investigación de este problema trascendental al repercutir en los ámbitos fiscal, social, de salud y seguridad pública, hacen falta herramientas e instrumentos adecuados para contrarrestar esta realidad virtual ya instituida en nuestra realidad material e histórica, y no tiene que ser disímbola ni se debe soslayar, sino que debe priorizarse y ser analizada minuciosamente con una óptica apegada a dichas características.

Señalaba Immanuel Kant, en cita por Décary *et al*. (2017), que las afirmaciones metafísicas por principio escapan a toda experiencia sensible, entendiendo por metafísica esas ideas básicas que se tienen del mundo como en su existencia como objeto, entidad, tiempo o espacio. Contexto en el cual han proliferado los mercados ilegales "*on line*", y donde en un inicio la primera generación de delitos cibernéticos no los alcanza.

Según estos mismos autores Décary *et al*. (2017), se desarrolla una actividad mercantil ilícita en todo el mundo donde haya internet, y los elementos personales pueden comprar y vender una amplia gama de bienes y servicios, como drogas, servicios de piratería informática, e información financiera robada, fraude financiero y fraude de propiedad intelectual. Pero estos delitos ya regulados en ordenamientos sustantivos penales, son delitos cibernéticos de primera generación.

Pero en cuanto a la investigación a desarrollar, nos avocamos a los delitos cibernéticos de segunda generación, como el caso de los criptomercados como modelo de análisis comparativo y poder suponer en su momento que México requiere de nuevas estrategias y modelos de investigación y fiscalización ante esta latente problemática, la cual al momento es obsoleta y poco vanguardista, como explicaremos más adelante.

Método

Ahora bien, a efecto de llevar a buen puerto esta investigación, bajo una metodología de problemas perversos y de análisis cualitativo, comparativo, teórico y documental, se hizo la revisión de literatura académica, informes institucionales (UNODC, Europol, OECD) y análisis de marcos normativos para diagnosticar la situación en México.

Y, de forma comparativa se estudiaron las estrategias internacionales de combate al comercio de drogas en línea, específicamente el caso de los *criptomercados en Estados Unidos y Europa* (ej. Operación Onymous) y las políticas de *control sobre la infraestructura de internet en China y Rusia*, para analizar su posible aplicabilidad y adaptación al contexto mexicano, que se caracteriza por un modelo híbrido basado en redes sociales.

Lo anterior con la perspectiva de diagnosticar la insuficiencia del marco jurídico fiscal mexicano para regular y fiscalizar el comercio electrónico de drogas ilícitas, por lo que para contrarrestar la actividad mercantil ilícita de drogas en línea, se observó en casos de Silk Road 1 y 2 por parte de Estados Unidos y algunos países de Europa, así como políticas chinas y rusas, una posibilidad.

Una de las estrategias significativas en la historia del combate a los mercados ilícitos de drogas en línea, acotados en los criptomercados, fueron algunas de las acciones emprendidas por Estados Unidos y algunos países de Europa a través de la Operación Onymous de 2014, analizada previamente en la justificación de estudio de los criptomercados, intervenidos éstos por parte de los servicios de inteligencia de los países participantes.

Lo anterior para establecer una propuesta para contrarrestar el comercio electrónico ilegal de drogas en línea, para que a través de una comparativa de las características de los mercados ilícitos en línea de los países donde ya se han implementado en criptomercados, analizar la posibilidad para implementarla en México, ésta no adaptada a la sofisticación de los pagos con monedas virtuales sino a buscar el control a través de la regulación de las redes sociales.

En relación con las redes sociales convendría observar a Rusia, que de acuerdo con Duffy (2016) lleva a cabo campañas para obtener el control completo sobre el acceso y la actividad del país a Internet; principalmente en contra de las posturas antigubernamentales, medidas con el objeto de detener la escalada de movimientos con esas características que presenten algún riesgo para el orden público y el concepto de éste en aquel país.

El presente análisis comparado es orientado a México y a la economía subterránea digital gestada en los mercados ilícitos de drogas en línea y los antecedentes internacionales a partir de 2014, que se estableció o que se ejecutó Onymous, antecedente inmediato que como ya se mencionó, el hallazgo de éste representa una posibilidad para contrarrestar el ilegal comercio electrónico de drogas en línea, en México.

Por lo que a través de este método de análisis cualitativo, comparativo, teórico y documental se demostrará que la situación actual de estos mercados ilícitos rebasa totalmente la comprensión y sensibilidad del Estado ante esta problemática que trasciende en los ámbitos de la economía, de la salud y seguridad pública como consecuencia de esa falta de dinamismo por parte de los órganos de gobierno de México, y más aún en esta era de los "*e governments*".

El problema en México

En México se ha observado que el combate al narcotráfico por lo menos hasta 2018 ha sido una estrategia frontal, en la cual busca contrarrestar al crimen organizado a través de la debilitación de la oferta o la demanda, es decir, incautaciones de la diversidad de drogas existentes o criminalizando a usuarios, por mencionar algunas, pero el problema que se suscita precisamente es que esta estrategia solamente ha desplazado a la oferta y demanda hacia mercados ilícitos cerrados.

Los mercados ilícitos de drogas a través de las "ventas en línea", han sofisticado los canales de distribución y establecido mercados fuera del alcance controlador del Estado, ya que en la República Mexicana a nivel estatal y federal los delitos informáticos que se persiguen son de primera generación, como el robo de identidad, fraude financiero, servicios de piratería informática, fraude de propiedad intelectual y, principalmente, el acoso cibernético.[3]

Aunado a lo anterior, y para poder visualizar la deficiente e ineficaz labor de seguridad en materia cibernética en delitos de segunda generación, podemos inferir el grado de ésta a partir de que no existe una legislación digital adecuada, un ataque informático no está contemplado como delito, salvo los considerados delitos informáticos ya mencionados; ejemplo de lo anterior, faltas menores como el robo de *wifi* no cuentan con una sanción.

Es decir, en México en el Código Federal Penal se contemplan la mayoría de los delitos informáticos en el Título Noveno, denominado: "Revelación de secretos y acceso ilícito a sistemas y equipos de informática". Asimismo, otros artículos dispersos también sancionan conductas delictivas a través de medios digitales; por ejemplo: de los artículos 211 bis 1 al 211 bis 7 Acceso y Daño a Sistemas Informáticos (H. Congreso de la Unión, 2025).

O bien, asociado con la Ley Olimpia, el delito de violación a la intimidad sexual (artículos 199 octies al 199 decies también del Código Penal Federal) que sancionan a quien divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona mayor de edad sin su consentimiento. O el de contacto con menores o "*grooming*" regulado en el artículo 199 septies, solicitan material de connotación sexual o encuentros.

Por lo que respecta al Código Penal en el estado de Jalisco, contempla delitos como obtención y uso ilícito de información (artículos 143-bis al 143-quáter), violencia digital

3 Insultos electrónicos, hostigamiento, denigración, suplantación, sonsacamiento, exclusión, ciber persecución o el *happy slapping* (que consiste en la grabación de una agresión física, verbal o sexual y su difusión *online* mediante las tecnologías digitales).

de género (artículos 176-bis 2 y 176-bis 3), o corrupción de menores (artículo 142-A) (Congreso del Estado de Jalisco, 2024). Ambos códigos castigan "*hacking*",[4] sin embargo en jalisco tipifica delitos como la suplantación de identidad y el ciberacoso en artículos específicos.

Con base en lo anterior y la evidencia normativa, material e histórica en el caso de México, como un hecho notorio podemos afirmar que no existe una legislación digital adecuada para contrarrestar el comercio electrónico en el mercado de drogas ilícitas en línea o implementar su fiscalización, en este caso desde una arista de seguridad pública a través de las fiscalías previo al trabajo legislativo en el rubro de delitos cibernéticos de segunda generación.

Por lo tanto, es pertinente preguntarnos: ¿cuál es el verdadero efecto de las estrategias actuales de seguridad cibernética en México? Ante ello, es primordial diagnosticar la insuficiencia del marco jurídico fiscal mexicano para regular y fiscalizar el comercio electrónico de drogas ilícitas y la migración de estos mercados a plataformas digitales y la generación de una economía subterránea que erosiona la base gravable y genera flujos de riqueza no fiscalizables.

De igual forma, en esta investigación se busca exponer el efecto de las estrategias al combate de los mercados ilícitos de drogas en línea, y cómo las estrategias tradicionales vigentes no fortalecen a esta economía digital. Por lo tanto, la hipótesis es que el verdadero efecto de las estrategias actuales de seguridad cibernética en México, antes que mitigar y dar solución al problema de forma gradual o integral, sólo fortalecen e incrementan estos mercados ilícitos de drogas en línea.

¿Por qué analizar criptomercados internacionales en el combate a mercados ilícitos de drogas en línea?

El realizar el estudio de este tópico es guiado esencialmente por la necesidad del estudio de la fiscalización del comercio electrónico internacional, esto orientado a los mercados ilícitos de drogas en línea como una premisa mayor. Es necesario mencionar que la aportación a la literatura mexicana servirá para analizar la fiscalización de los criptomercados como un medio para contrarrestar los negocios digitales ilícitos.

En el caso de los criptomercados analizados en Europa y Estados Unidos, cuentan con un modelo que nos actualiza y que debe despertar del letargo e ineficiencia legislativa y valorar su factibilidad en la implementación en México, tomando en cuenta las características de los criptomercados, los cuales hacen su aparición en 2011 caracterizados por plataformas seudo anónimas, como el caso de Silk Road 1 o SR1.

Fenómeno que ha atraído la atención de investigadores, reguladores y agentes de la ley, y que en este trabajo buscamos aportar a esa línea de investigación vigente en economía digital, ante la virtualidad aprovechada tanto por la delincuencia organizada como por los usuarios de dichos bienes y servicios demandados y no así por el Estado en su labor gubernativa, fiscalizadora, o bien, recaudatoria ante una parcial[5] legalización de la mariguana en México con el CBD, por ejemplo.

Asimismo, es importante poner manos a la obra ante el crecimiento de los mercados de drogas virtuales y en línea, que plantea importantes desafíos para las políticas de aplicación de la ley y control de drogas. Además de la necesidad de conceptualizar la integración de esta dimensión cibernética en todos los aspectos relevantes del trabajo policial, y motivar con nuestro trabajo de investigación el diseño de una estrategia y un plan de implementación para que esto suceda.

Además, la importancia de analizar que las intervenciones policiales pueden llevar a un cambio de mercados de drogas "abiertos" a "cerrados", con distribuidores que pueden adoptar soluciones tecnológicas como teléfonos celulares y aplicaciones de mensajería como Telegram o Signal que usan cifrado de extremo a extremo y sirven para contactar a sus proveedores y clientes de manera encubierta y evadir la vigilancia, o mediante la privacidad de las redes sociales.

Incluso de acuerdo con Noriega (2022), las redes además han servido esa falta de fiscalización, para que los cárteles mexicanos, especialmente el Cártel Jalisco Nueva Generación (CJNG), utilicen plataformas lícitas como Facebook, TikTok e Instagram como herramientas activas de reclutamiento forzado a través de publicación de ofertas de trabajo engañosas que prometen empleos bien remunerados como encuestadores, escoltas o guardias de seguridad.

Los jóvenes que responden a estos anuncios son citados en un lugar y luego llevados a campos de entrenamiento del cártel, donde son obligados a trabajar para la organización bajo amenaza de muerte. Este método valida directamente el argumento del "modelo híbrido", ya que demuestra cómo el crimen organizado aprovecha la infraestructura de plataformas digitales de uso masivo para ejecutar operaciones criminales (reclutamiento) que se materializan en el mundo físico.

Con base en esta situación, que no hemos comprendido que debemos estar a la par de esta evolución, como en el caso de China, donde por ejemplo de 1999 a 2001 de acuerdo con Harwit (2001):

4 El acceso ilícito a sistemas.

5 Parcial porque sólo se ha legalizado la marihuana medicinal desde 2017 y reglamentada desde enero de 2021 con base en el *Diario Oficial de la Federación.*

> [...] el ancho de banda internacional de datos del país se ha expandido en un factor de 20 y más de 300 ciudades obtuvieron conexiones de alta velocidad a la red. A principios de 2001 había unos 1,500 sitios web de comercio electrónico [...] la evolución demográfica de los usuarios de Internet y las formas en que se transfiere la información dentro de la sociedad china también están dando forma a las actitudes del Gobierno hacia la regulación de la autopista de datos.

Asimismo, señala también Harwit (2001) que China a través de tres pilares intenta controlar no sólo mercados ilícitos sino todo el espectro virtual:

> *Primero,* discute el control físico de la red, preguntando quién construyó las tuberías de datos reales a través de las cuales fluye la información, y quién ahora regula y se beneficia de estos sistemas. ¿Y cómo compiten las diferentes partes del Gobierno y del sector privado por el control de la infraestructura de la red?
>
> *En segundo lugar*, examinamos el control de contenido de la red. ¿Quién puede publicar y enviar información a través de la red y qué límites políticos se colocan en este contenido? ¿Qué dinámica del Gobierno / sector privado afecta la competencia para el público web y cómo afectan los flujos de ingresos a las empresas proveedoras de contenido? ¿Cómo la demografía de los usuarios determina el contenido, y cómo la reacción del usuario al contenido da forma a los patrones sociológicos que, a su vez, influyen en el grado de control del Gobierno sobre lo que aparece en las pantallas de las computadoras?
>
> *Finalmente*, también consideramos el elemento de influencia extranjera en la red: ¿cómo afecta el contenido web extranjero a los espectadores chinos y cuáles son las perspectivas de cambio en el futuro cercano? ¿Cómo afectará la entrada de China en la Organización Mundial del Comercio (OMC) a la participación extranjera en la gestión de la red física?

O Rusia, que lleva a cabo campañas para obtener el control completo sobre el acceso y la actividad del país a Internet; lo anterior en contra principalmente de las posturas antigubernamentales, o como lo señala la propia literatura con Duffy (2016), que proponen un "interruptor de muerte" que permitiría al Gobierno cerrar Internet en Rusia durante desastres definidos por el Gobierno, incluidas protestas civiles a gran escala… campañas de opresión, etcétera.

Lo anterior en cuanto a las restricciones dentro del ciberespacio, y en un entorno de debate, ante la violación a derechos fundamentales, como el del uso de internet como un derecho humano, países en los cuales antes que olvidar este tema de la virtualidad, la evolución de la red ha ido ligada al control político sobre la infraestructura de red y contenidos, pero que en el tema que nos ha traído a esta investigación estas medidas de control serían muy importantes.

Ahora bien, en una visión cuantitativa de acuerdo con Aldridge (2016), por ejemplo:

> El FBI estimó que las ventas totales en SR1 (Silk Road 1)[6] de febrero de 2011 a octubre de 2013 estuvieron en el rango de $200 millones de dólares. Esto se traduce en aproximadamente $80 millones de dólares en promedio por año, una cifra cercana a la proporcionada por los investigadores académicos. Esto marca un fuerte aumento de la estimación de 2012 de $14.4 millones de dólares por parte de Christin, quien utiliza una metodología similar a la utilizada por Allen y Décary-Hétu, pero representa mucho menos del 1% del tráfico total de drogas ilícitas. Hasta el momento, el 2 de octubre de 2013, el primero de ellos, el 2 de octubre de 2013 provocó el cierre de SR1 por parte de las fuerzas del orden público de EE.UU., la incautación de más de $33 millones de dólares en bitcoins y el arresto de su fundador y administrador. Los participantes de SR1 se movieron rápidamente a otros criptomercados, incluidos Agora, Cloud-Nine, Evolution, Hydra, Sheep y Silk Road 2 (SR2). Varios de estos criptomercados estuvieron activos por poco tiempo, ya que fueron retirados durante una segunda operación policial, la "Operación Onymous" lanzada el 5 de noviembre de 2014.

Asimismo, un dato significativo del Informe mundial sobre las drogas 2023 de la UNODC (2023) es la drástica reducción de los ingresos en los mercados de drogas de la red oscura *(dark web)* durante 2022, tras alcanzar un máximo histórico el año anterior. Específicamente, los ingresos combinados de los principales mercados de la red oscura, que en su mayoría venden drogas, alcanzaron un récord de 2,700 millones de dólares en 2021.

Posteriormente hubo un fenómeno en el cual cayó a la mitad, a unos 1,300 millones de dólares en 2022. Esta disminución en la *dark web* coincide con una tendencia creciente en el uso de plataformas de redes sociales convencionales y aplicaciones de mensajería cifrada para la venta de drogas, lo que fragmenta y localiza el mercado, haciéndolo más accesible para un público más amplio, que es propiamente el fenómeno que planteamos.

Por otra parte, en alusión a los diversos criptomercados, de acuerdo con el Informe de evaluación de la amenaza de la delincuencia organizada en Internet (IOCTA) (2023) por parte de Europol, tras el desmantelamiento del mercado de la *darknet* Hydra Market en abril de 2022 (el más grande y duradero hasta la fecha) no ha surgido un sucesor dominante. En su lugar, la principal amenaza y táctica de adaptación del crimen organizado ha sido la fragmentación del ecosistema.

6 Primer "criptomercado", un sitio web clandestino que se asemejaba a plataformas de comercio electrónico como eBay o Amazon, pero que se dedicaba a la venta de bienes y servicios ilícitos.

Los vendedores y compradores de Hydra se dispersaron hacia múltiples mercados más pequeños y competidores, como OMG!OMG!, Blacksprut, Mega, Solaris y WayAway. Esto representa un nuevo desafío para las fuerzas del orden, ya que la ausencia de un mercado centralizado complica el monitoreo y las investigaciones, obligando a las agencias a adaptar sus estrategias para hacer frente a una amenaza más descentralizada y distribuida.

Por lo tanto, la implementación de diversas estrategias en el combate de los mercados ilícitos de drogas en línea y la migración de los mercados en México a la virtualidad requiere acciones inmediatas, y deberá ser muy importante para los órganos de seguridad pública de los distintos órdenes de gobierno los recursos tecnológicos y servicios de inteligencia adecuados en beneficio de todos mediante herramientas de fiscalización necesarias para esta realidad virtual.

Cabe señalar que el presente trabajo, aunque se basa en estrategias a partir del combate a los criptomercados, como fachada de los mercados ilícitos de drogas en línea, nuestra aportación será basal a la realidad mexicana a partir del mercadeo en redes sociales, tema que no se toca en la literatura revisada el conducir su objeto de análisis a las monedas virtuales, analogía que se busca establecer para buscar una mejor perspectiva de la problemática en México.

Fundamentos

En primera instancia, de acuerdo con Buxton *et al*. (2015) se debe entender el término de "mercados abiertos" de venta de drogas como lugares específicos donde generalmente los usuarios de diversos estupefacientes[7] van a comprar drogas ilícitas y se caracterizan por un mayor riesgo (tanto de aplicación como de violencia), ya que los compradores tratan con los distribuidores que están disponibles en ese momento y en ese lugar, en vez de hacerlo con un concesionario que ya conocen.

Situación que cobra relevancia, ya que dentro de la hipótesis de que el verdadero efecto de las estrategias actuales de seguridad cibernética en México, antes que mitigar y dar solución al problema de forma gradual o integral, sólo fortalecen e incrementan estos mercados ilícitos de drogas en línea, ya que la actuación policial ante el decomiso a consumidores y/o usuarios los criminaliza e incrementa el riesgo para obtener el bien, lo cual orilla al consumidor a la virtualidad.

O bien, parafraseando a Aldridge (2016), la ineficacia para frenar el tráfico de drogas en México a través de una economía digital encuentra eco en el desplazamiento geográfico, que es otra forma común de adaptación a las operaciones policiales. Varios estudios han demostrado que las represiones policiales no pueden reducir la cantidad de transacciones, pero pueden conducir a un cambio en la ubicación física donde se encuentran los distribuidores y los usuarios.

Se asevera además, ya que por observación directa del mercado al que hacemos alusión, empíricamente hemos comprobado que el consumo de drogas en México está migrando a mercados cerrados que permiten salir del radar de la autoridad a través de la plataformas digitales y medios de distribución personalizados no de estante sino de reparto, utilizando "Uber flash" o equipo de reparto del propio comerciante ante la percepción del riesgo por parte del consumidor.

Entiéndase entonces a los mercados cerrados como el punto de encuentro entre la oferta y la demanda que se da de forma exclusiva entre vendedor y comprador, en la cual interviene un espacio digital privado para disminuir la percepción del riesgo del cliente y la seguridad del proveedor ante la ilegalidad de éste y de los bienes y servicios que proporciona, mismos que se individualizan en espacios generalmente bilaterales o grupales de venta.

Atendiendo a nuestra perspectiva principal y la idea a contrastar con la realidad mexicana, esto a partir de los criptomercados, los definen Décary *et al*. (2016) dentro del espectro que se estudia, como:

> [...] sitios web que permiten a los participantes comprar y vender bienes y servicios a la vez que proporcionan cierto nivel de anonimato. Sus actividades se centran en la venta de drogas lícitas vendidas ilícitamente (medicamentos recetados) y la venta de drogas ilícitas (cannabis, estimulantes, nuevas sustancias psicoactivas). Estas tecnologías protegen la identidad de los participantes al enrutar todo su tráfico a través de la red Onion Router, lo que hace que sea muy difícil encontrar la dirección IP de los participantes, así como la dirección IP de los servidores que alojan los criptomercados. El anonimato de los participantes se ve reforzado por el uso de bitcoins como método de pago para las compras.

A lo anterior y para dar un panorama más completo al respecto en este tema, se transcribe un fragmento de la historia de dichos criptomercados:

> El primer criptomercado fue Silk Road (SR1), que saltó a la fama a través de las noticias de 2011 de GawkerMediat que describieron "el sitio web subterráneo donde puedes comprar cualquier droga imaginable". La figura 1 muestra la página principal de SR1, que se asemeja a sitios web de comerciantes lícitos como eBay y Amazon.

7 Dicho de una sustancia: que altera la sensibilidad y puede producir efectos estimulantes, deprimentes, narcóticos o alucinógenos, y cuyo uso continuado crea adicción.

> Los países europeos y los EE. UU. llevaron al arresto de 17 personas, incluido el administrador de SR2. También condujo a la incautación de más de $1.3 millones de dólares en bitcoins, efectivo, metales preciosos y drogas. En el momento de la Operación Onymous, los criptomercados con la mayor cantidad de listados (el nombre en línea de una página de producto y un proxy del tamaño y relevancia de los criptomercados) eran, en orden, Agora, SR2, Evolution, Andrómeda, Bluesky, Cloud-Nine e Hydra.
>
> La primera técnica de desplazamiento utilizada por los participantes fue moverse virtualmente a nuevos criptomercados. Después del cierre de SR1, muchos participantes se mudaron a Black Market Reloaded (BMR) y Sheep. En las 6 semanas posteriores al cierre de SR, BMR experimentó un doble aumento en el número de distribuidores; El número de distribuidores de Sheep se multiplicó por más de cuatro. Buxton y Bingham describen un desplazamiento geográfico virtual similar de participantes después de la Operación Onymous, con una actividad en Agora y Evolution que aumenta en las semanas siguientes (Décary *et al*., 2017).

Por su parte, Soska *et al*. (2015) en su estudio de "la evolución longitudinal del ecosistema del criptomercado", establece la resistencia tanto a las estafas como al cierre; además, muestran que poco después del desmantelamiento de Silk Road 1 y 2, BMR absorbió una gran parte de las ventas, lo que indica el cambio de vendedores y compradores al nuevo criptomercado, es decir cada vez más compleja su extinción.

Por el contrario, por parte de la Operación Onymous afectó significativamente las ventas en el sistema de criptomercado, aunque las ventas en Evolution y Agora comenzaron a crecer rápidamente después de algunas semanas de la intervención policial. Por lo tanto, se denota este negocio virtual y de economía digital como un negocio a corto plazo por la facilidad del manejo de información en cuanto a la nomenclatura y anonimato de los participantes.

Situación que permite ese desplazamiento ya no sólo físico, sino ante la facilidad del tiempo y espacio que permite la internet. Además, del análisis de la información, ni el estado ni sus estrategias son el enemigo o la némesis de estos negocios virtuales, sino propiamente el crecimiento y la popularidad de estos mercados, al ser de corta duración, su obstáculo principal es el crecimiento de la desconfianza entre los participantes del mercado debido a estafas.

Ahora bien, con base en Aldridge *et al*. (2016), en la actualidad los criptomercados representan sólo una pequeña fracción del tráfico mundial de drogas y se han centrado dichas estrategias en los criptomercados, ya que los mercados de criptomonedas pueden proporcionar a los investigadores de datos la necesidad de observar los patrones de uso y la penetración de drogas en países de todo el mundo.

De acuerdo con Aldridge *et al*. (2016), los criptomercados emplean una variedad de estrategias para ocultar las identidades de sus participantes, realizar transacciones anónimas y ocultar las ubicaciones físicas de los servidores. Pero ¿cómo logran este fin? A partir de servicios de anonimización,[8] como el Tor (The Onion Router), que oculta la dirección IP de una computadora cuando accede al sitio.

Dentro de este mar conceptual de contexto teórico, algunos otros como Barratt (2012) y Martin (2013) emplean el término "criptomercados" luego del uso temprano de este término en foros de piratas informáticos, pero al igual que el anterior, también el término "mercados netos oscuros" está ganando vigencia en cita de Buxton *et al*. (2015). Con lo cual el antecedente de los criptomercados es el punto de partida ideal para tratar de contener el problema planteado.

Conclusión

En esta investigación se ha demostrado que las estrategias tradicionales y frontales del Estado mexicano contra el narcotráfico resultan contraproducentes en el entorno digital. Al centrarse en la materialidad del delito, estas políticas han incentivado el desplazamiento de la oferta y la demanda hacia mercados cerrados en línea en redes sociales, consolidando una economía subterránea que erosiona la base gravable y opera fuera del alcance fiscal y judicial del Estado.

Se comprueba así la hipótesis de que el enfoque actual, lejos de mitigar el problema, fortalece e incrementa estos mercados ilícitos. El análisis de experiencias internacionales, como el desmantelamiento de criptomercados[9] y las operaciones policiales a gran escala como el programa Onymous, revela una lección fundamental: aunque sus efectos han sido a corto plazo, demuestran la capacidad de los Estados para intervenir directamente en los ecosistemas digitales ilícitos.

Del mismo modo, aunque modelos de control como los de China y Rusia son a menudo considerados arbitrarios y plantean debates sobre derechos fundamentales, ofrecen un paradigma de gobernanza digital proactiva. En lugar de tratar el ciberespacio como un territorio ingobernable, lo abordan como una extensión de su soberanía, aplicando un control riguroso sobre la infraestructura de red y sus contenidos.

La propuesta para México no es replicar estas medidas de forma idéntica, sino adaptar su principio fundamental a nuestro contexto democrático: el Estado debe afirmar su

8 O criptomonedas descentralizadas y relativamente imposibles de rastrear, como bitcoin y litecoin, para realizar pagos; y comunicación encriptada entre los participantes del mercado.

9 Silk Road 1 es el pionero.

autoridad regulatoria y fiscal sobre las plataformas digitales que, aunque lícitas, sirven como vehículo para el comercio ilícito de drogas. A partir de esta premisa se proponen las siguientes líneas de acción:

1. *Reforma jurídica para la fiscalización y sanción del comercio ilícito en plataformas lícitas*. Actualizar el marco legal para tipificar de manera explícita el "narcomenudeo digital" realizado a través de redes sociales y aplicaciones de mensajería. Esta legislación debe contemplar la responsabilidad solidaria de las plataformas que operan en México, obligándolas a implementar mecanismos proactivos de detección, colaboración y reporte.
2. *Adaptación de tácticas de intervención digital*. Inspirado en la lógica de operaciones como Onymous, se debe formar una fuerza de tarea de ciberinteligencia que integre a la unidad de inteligencia financiera (UIF) al SAT, a la Guardia Nacional y a la FGR. Su mandato sería desmantelar proactivamente las redes de comercio de drogas en plataformas lícitas, "siguiendo el dinero" desde la transacción digital hasta la cuenta bancaria.
3. *Gobernanza estratégica de la infraestructura digital*. Tomando como referencia funcional los modelos de control de China —pero sin adoptar sus aspectos autoritarios—, México debe establecer una política de soberanía digital, crear un marco regulatorio que permita auditar los algoritmos de las plataformas para prevenir la proliferación de mercados ilícitos y exigir el cumplimiento estricto de la ley mexicana como condición para operar en el país.

Con base en lo anterior, podemos concluir y coincidimos en que los participantes de los criptomercados se adaptan a las operaciones policiales rápidamente y que el impacto de operaciones como Onymous fue limitado en tiempo y alcance. Asimismo, las operaciones policiales desplazan a los participantes a mercados alternativos de drogas en línea, pero no limitan sus actividades, por el contrario, incentivan la creación de mercados cerrados.

Por otra parte, se ha demostrado que los participantes de criptomercados tienen una reacción mínima, o una que es temporal, a manifestaciones de fuerza abiertamente grandes y tienen la capacidad de adaptarse a través de técnicas de desplazamiento; lo anterior, ante el modelo de riesgos y precios de Reuter y Kleiman supone que la compensación por los costos no monetarios es el factor principal que eleva el precio de las drogas ilícitas de acuerdo con Décary *et al*. (2017).

Asimismo, el modelo de estrategias utilizada en los criptomercados tampoco es un modelo ideal a largo plazo, ya que por la evidencia existente, estas acciones sólo provocan o establecen resultados a corto plazo, ya que las características propias de comercio electrónico ante la facilidad del desenvolvimiento en tiempo y espacio con mayor facilidad, así como un modelo de riesgos y precios no reducen ni mitigan los números que resultan de tales acciones policiales.

Por lo que México, deberá ser consciente de la problemática existente, primero el legislar al respecto, aceptar la realidad virtual que se vive y la economía subterránea como punto de partida hacia los delitos de segunda generación en los cuales este país no ha tipificado la conducta penalmente, con lo cual se cumple con el objetivo trazado al exponer a través del análisis el efecto de las estrategias al combate de los mercados ilícitos de drogas en línea.

De igual forma, las estrategias tradicionales vigentes no fortalecen a esta economía digital, y con lo cual para el caso México serviría aún más ejercer controles sobre la infraestructura de la red y sus contenidos, como en el caso de China, que por cierto parte de su poderío económico está basado también en estas tecnologías de la información a partir de su entendimiento y un análisis más profundo de esta cultura cibernética y de innovadoras inteligencias.

Por lo tanto, México debe reconocer que la inacción es una forma de ceder el control del espacio digital al crimen organizado. La solución no reside en ignorar las estrategias internacionales por considerarlas extremas, sino en adaptar de forma inteligente sus principios de intervención y control a la realidad de un mercado que utiliza plataformas legales para fines ilegales.

Sólo así el Estado podrá recuperar su soberanía fiscal y reafirmar su autoridad en la economía digital del siglo XXI.

Referencias bibliográficas

Martin, J. (2014). *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs.* Reino Unido: Palgrave, Macmillan.

Tapscott, D. (1997). La economía digital: Las nuevas oportunidades y peligros en un mundo empresarial y personal interconectado en red. *La economía digital: Las nuevas oportunidades y peligros en un mundo empresarial y personal interconectado en red* (p. 323). Santafé de Bogotá: McGraw-Hill.

Referencias hemerográficas

Aldridge, J., & Décary Hétu, D. (2016). Cryptomarkets and the future of illicit drug markets. *European Monitoring Centre for Drugs and Drug Addiction* (pp. 23-30). https://doi.

org/10.2810/324608 Obtenido de https://www.academia.edu/75316167/Cryptomarkets_and_the_future_of_illicit_drug_markets?uc-g-sw=72117083 [consulta julio de 2022].

Buxton, J., & Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory* (pp. 2-19).

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *International World Wide Web Conference Committee (IW3C2)* (pp. esta versión: noviembre 28, 2012). Río de Janeiro, Brazil/ Pittsburgh, PA: Carnegie Mellon University.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime Law Soc Change*, pp. 55-75.

Harwit, E., & Clark, D. (2001, junio). Shaping the Internet in China, Evolution of Political Control over Network Infrastructure and Content. *University of California Press, XLI*(3), 377-408.

Noriega, R. (2022). *How Mexico's brutal cartels are taking over social media. American Enterprise Institute (AEI)*. https://www.aei.org/op-eds/how-mexicos-brutal-cartels-are-taking-over-social-media/

Sotres Arévalo, S. G. (2010). La empresa virtual, un nuevo esquema de negocios en la red. *Revista Digital Universitaria, 11*(10).

Consultas en sitios de Internet

Duffy, N. (2016). *Libertad de Internet en la Rusia de Vladimir Putin: La soga se tensa.* Obtenido de https://www.questia.com/:https://www.questia.com/library/journal/1G1-414680951/internet-freedom-in-vladimir-putin-s-russia-the-noose

Excélsior. (2019, 03 de noviembre). Cómo denunciar delitos cibernéticos en México. *Excélsior*. Obtenido de https://www.excelsior.com.mx: https://www.excelsior.com.mx/hacker/como-denunciar-delitos-ciberneticos-en-mexico/1311256

Real Academia Española. (2019). *Cibernético, ca*. Obtenido de https://dle.rae.es: https://dle.rae.es/?id=98yyoxw

Soska , K., & Christin, N. (2015, 12 de agosto). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.* Obtenido de https://www.usenix.org: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

Referencias institucionales, leyes y jurisprudencia

Congreso de la Unión. (2025). *Código Penal Federal*. Cámara de Diputados. Obtenido de https://www.diputados.gob.mx/leyesbiblio/pdf/cpf.pdf [consulta septiembre de 2025].

Congreso del Estado de Jalisco. (2024). *Código Penal para el Estado Libre y Soberano de Jalisco*. https://congresojal.gob.mx/bibliotecavirtual/legislacion/vigente [consulta septiembre de 2025].

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. Oficina de Publicaciones de la Unión Europea. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%202023.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2023). *World Drug Report 2023*. Naciones Unidas. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html

Organización para la Cooperación y el Desarrollo Económico (OCDE). (2020). *Taxing the Digital Economy: An assesment of the options*. OECD Publishing. https://www.oecd.org/tax/beps/taxing-the-digital-economy-an-assesment-of-the-options.pdf

UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS ECONÓMICO ADMINISTRATIVAS