

# LA VERDAD SOBRE LA WEB OSCURA

Tiene la intención de proteger a los disidentes, pero también permite ocultar actividades ilegales

**Aditi Kumar y Eric Rosenbach**

**A** fines de los años noventa, dos centros de investigación del Departamento de Defensa de Estados Unidos lideraron los esfuerzos por crear una red anónima y encriptada que protegería las comunicaciones sensibles de los espías de ese país. Los usuarios comunes de Internet no se enterarían de su existencia ni tendrían acceso a ella. Y aunque la intención secreta original nunca se materializó del todo, algunos investigadores divisaron una propuesta de valor distinta: crear un organismo sin fines de lucro para proteger el anonimato de activistas que abogan por la privacidad y los derechos humanos.

Nace la red Tor (según iniciales de “The Onion Router”, es decir “router cebolla”, por las múltiples capas que encriptan los datos en tránsito). Parte de la periferia de Internet, Tor es la tecnología que posibilita la “web oscura” (conjunto de sitios ocultos e inaccesibles para los navegadores comunes y que motores de búsqueda como Google no indexan). Con el buscador Tor —de descarga gratis— cualquiera accede a este rincón de la web donde la privacidad es primordial. La sombra de este anonimato extremo, sin embargo, es larga.

La verdad es que además de ofrecer un alto grado de privacidad y protección frente a la vigilancia de gobiernos autoritarios, la web oscura facilita un creciente mercado clandestino que delincuentes astutos emplean para traficar drogas, identidades robadas, pornografía infantil y otros productos y servicios ilícitos. Y dado que el principal medio de pago es a través de criptomonedas indetectables, se requiere una estrecha colaboración de las fuerzas del orden, las instituciones financieras y los organismos reguladores del mundo entero para combatir esta nefasta actividad.

## Las zonas grises

Hoy, la red Tor reúne a más de 65.000 Localizadores Universales de Recursos (URL) únicos que emplean la terminación “.onion”. Un estudio de 2018 de la empresa de seguridad Hyperion Gray clasificó a un 10% de estos sitios y determinó que sus funciones más comunes facilitan la comunicación a través de foros, “chats”, servicios de carga de archivos e imágenes, así como el comercio virtual. Estas funciones, sobre todo las del ámbito de las comunicaciones, respaldan muchos usos considerados legales y legítimos en sociedades libres. Asimismo, según un estudio de 2016 de



la empresa de investigación Terbium Labs que analizó 400 sitios escogidos al azar con la terminación “.onion”, más de la mitad de los dominios de la web oscura son en realidad legales.

Para los que viven en regímenes opresivos que bloquean gran parte de Internet o castigan la disidencia política, la web oscura es una vía de escape que brinda acceso a información y protege de la persecución. En sociedades más libres, es una herramienta esencial de comunicación y denuncia de irregularidades que protege a las personas de represalias o censura en su lugar de trabajo o comunidad. Por otra parte, ofrece privacidad y anonimato a los que se oponen a la forma en que empresas y gobiernos vigilan, emplean y monetizan sus datos. Actualmente, muchos organismos, todos los principales periódicos, Facebook e incluso la CIA mantienen sitios ocultos en la red Tor porque hacerlo demuestra (a veces simbólicamente) un compromiso con la privacidad. Para el *New York Times* y la CIA, por ejemplo, la idea es facilitar una comunicación virtual accesible para cualquiera que pueda proporcionar información sensible.

La otra cara de la moneda es que esa misma privacidad y anonimato que brindan protección contra tiranos y avisos publicitarios focalizados en determinados grupos convierten a la web oscura en una plataforma para la delincuencia. Las actividades ilícitas más comunes incluyen el tráfico de armas, la venta de drogas y la distribución de pornografía, imágenes de violencia, así como de otros tipos de abuso, que a

**Para los que viven en regímenes opresivos que bloquean gran parte de Internet o que castigan la disidencia política, la web oscura es una vía de escape.**

menudo involucran la explotación de niños. Hay sitios web que apoyan el discurso de neonazis, supremacistas blancos y otros grupos extremistas.

Esta combinación de servicios de la web oscura y criptomonedas ha generado expectativas de un auge de la criminalidad. Hace 10 años, un criptógrafo desconocido (experto en descifrar contraseñas) que empleaba el alias Satoshi Nakamoto creó el bitcoin, la primera moneda y red de pago no sujeta a control estatal. Aunque al inicio se diseñó como medio de intercambio para la comunidad tecnológica, en 2011 el bitcoin se había convertido en la divisa preferida de narcotraficantes que comerciaban en un sitio de la web oscura llamado Silk Road. En los últimos cinco años, mediante la combinación de una red cifrada, oculta para la mayor parte del mundo, y una moneda de transacción prácticamente indetectable para las fuerzas del orden, se creó un pequeño pero importante mercado de vendedores de mercancía ilícita.



## Muchas de las amenazas más dañinas para la sociedad hoy se manifiestan en la sombra de la red Tor y, por lo tanto, deben ser examinadas por investigadores internacionales.

De los casi 200 dominios que Terbium Labs clasificó como ilícitos, más del 75% son, al parecer, mercados virtuales. Muchos de estos mercados operan con bitcoins y otras criptomonedas, como Monero. Las mercancías más comunes son drogas y fármacos, seguido por documentos de identidad, tarjetas de crédito y datos bancarios robados y falsificados. Algunos sitios ofrecen servicios de piratería y delincuencia tecnológica, como programas dañinos, herramientas de ataque de denegación de servicio distribuido, así como servicios de piratería por contrato. Un buen número ofrece un surtido de estos servicios además de pornografía y mercadería falsificada.

Aunque la gravedad y el rápido crecimiento de estas operaciones ilícitas en la web oscura deberían inquietar a las autoridades y las instituciones financieras mundiales, el comercio en esa red es minúsculo en relación con el comercio ilícito total a escala mundial. Según un estudio reciente de Chainalysis, una de las principales empresas de análisis de criptopagos, el volumen de transacciones de la web oscura realizadas con bitcoins aumentó de alrededor de USD 250 millones en 2012 a USD 872 millones en 2018. Según proyecciones de la empresa, en 2019 las transacciones en bitcoins en la web oscura alcanzarán más de USD 1.000 millones. Si esa proyección es correcta, el volumen de transacciones ilegales en este ámbito alcanzará un nivel sin precedentes. Asimismo, el informe señala que, desde 2012, la proporción de transacciones vinculadas a operaciones ilícitas realizadas con bitcoins ha disminuido 6% y actualmente asciende a menos del 1% de toda la actividad realizada con esa moneda. Según estimaciones más generales de las Naciones Unidas, el monto de lavado de dinero en todo el mundo representa entre el 2% y el 5% del PIB

mundial por año, es decir, entre USD 1,6 billones y USD 4 billones.

Aunque el volumen económico total de la actividad ilícita en la web oscura sigue siendo relativamente reducido, muchas de las amenazas más dañinas para la sociedad hoy se manifiestan en la sombra de la red Tor y, por lo tanto, deben ser examinadas a nivel internacional por organismos reguladores, instituciones financieras y entidades policiales.

### Patrullaje entre las sombras

Proteger a disidentes políticos, a quienes abogan por la privacidad y a denunciantes de irregularidades no debe ser a expensas de empoderar a pedófilos, traficantes de armas o narcotraficantes. Ese es precisamente el reto que enfrentan los organismos reguladores y las fuerzas del orden: cómo equilibrar la protección de principios liberales en una era de control de la información con la detección y erradicación de las actividades más insidiosas que se realizan en esa oscura trama. En los últimos años, la comunidad internacional ha logrado importantes avances en este frente, al mejorar el intercambio de información, ampliar la capacidad técnica de la policía para dismantelar mercados ilícitos, y regular la transferencia de transacciones en criptomonedas.

El primer paso para hacer frente a las actividades más nefastas de la web oscura es mejorar el intercambio de información entre las fuerzas policiales y las instituciones financieras. Dado el carácter mundial de dicha red, la cooperación internacional es esencial. En 2018–19, Interpol y la Unión Europea reunieron a las fuerzas del orden público de 19 países para identificar a 247 sospechosos de sumo interés e intercambiaron la información necesaria para poder aplicar la ley. Los resultados fueron prometedores: la

labor de este grupo solo en este año permitió detener a sospechosos y clausurar 50 sitios ilegales de la web oscura, como Wall Street Market y Valhalla, dos de los mayores mercados de drogas.

El auge de operaciones ilegales en la web oscura también ha incitado a las autoridades de muchos países a controlar la criminalidad mejorando la capacidad de entidades policiales nacionales como la Oficina Federal de Investigaciones de Estados Unidos (FBI). El FBI, por ejemplo, supuestamente ha realizado operaciones para “desanonimizar” los servidores de Tor estableciendo nodos en la red que le permiten ver la identidad y la ubicación de algunas páginas virtuales ilícitas en la red Tor. El primer acto importante en este sentido fue el desmantelamiento en 2014 del sitio Silk Road 2.0, el principal mercado virtual ilícito de la web oscura. La investigación reveló que, en dos años y medio de actividad, varios miles de traficantes de droga y vendedores ilegales habían recurrido al sitio para distribuir cientos de kilos de drogas y otros productos y servicios prohibidos a muchos más de 100.000 compradores. El sitio se utilizó para blanquear los cientos de millones de dólares provenientes de estas transacciones ilícitas. En total, el sitio generó ventas de más de 9,5 millones en bitcoins, equivalente en aquel entonces a unos USD 1.200 millones. AlphaBay y Hansa Market, dos de los principales sucesores de Silk Road, fueron desmantelados en 2017.

La capacidad para reprimir las actividades de la web oscura ha seguido desarrollándose: por ejemplo en una reciente operación de los Países Bajos se logró entrar en una conocida web oscura de un traficante, se la manejó en forma anónima por un mes, y así fue posible obtener información para detener a docenas de otros traficantes de la web oscura.

### Se requieren nuevas normas

Además de realizar operaciones de desmantelamiento, los gobiernos y los organismos internacionales están intentando regular directamente las criptomonedas que fomentan los mercados de la web oscura. En junio de 2019, por ejemplo, el Grupo de Acción Financiera

Internacional emitió directrices que instan a las empresas que procesan transferencias en criptomonedas a identificar tanto a sus remitentes como a sus beneficiarios. Estas directrices se ajustan a la recomendación de la reunión cumbre del G-20 de 2018, en la que se solicitó a las entidades reguladoras internacionales que consideraran medidas frente a los cryptoactivos, sobre todo en relación con el principio de conocimiento del cliente, la lucha contra el lavado de dinero y la prevención del financiamiento del terrorismo. El ecosistema de nuevas empresas que han creado mercados, billeteras y otros mecanismos que facilitan los criptopagos dista mucho de contar con la infraestructura necesaria para poder adoptar normas como las del sector financiero, pero los supervisores necesitan empezar por sentar las bases para supervisarlos mejor. Con el próximo lanzamiento de Libra, la criptomoneda de Facebook, esta tarea se volverá aún más apremiante ya que las barreras a la adopción de activos virtuales se reducirán para los más de 2.000 millones de usuarios de esa plataforma.

### Un equilibrio delicado

Los regímenes autoritarios seguirán intentando bloquear el acceso a la web oscura y las amenazas a su legitimidad que esta plantea al empoderar a disidentes y activistas. Frente a este peligro, el reflejo natural de las sociedades civiles liberales será abogar por que Tor siga exenta de supervisión y vigilancia policial para proteger la libertad de expresión y la privacidad. La realidad de la web oscura es mucho más compleja, exige de las entidades de supervisión y control un enfoque que impida actividades consideradas ilícitas e inmorales en sociedades libres, pero que a la vez proteja los genuinos beneficios de una red anónima. **FD**

**ADITI KUMAR** es director ejecutivo del Centro Belfer de Ciencia y Asuntos Internacionales de la Escuela de Gobierno John F. Kennedy de la Universidad de Harvard.

**ERIC ROSENBACH** es codirector del Centro Belfer y fue anteriormente Subsecretario de Defensa para la Seguridad Global de Estados Unidos.