DARK WEB: ¿UN REFUGIO O UN SUPERMERCADO DE VIOLENCIA?

Por: Axel Marazzi/ Tomás Pérez Vizzón. Revista Anfibia. 11/01/2018

Ser invisible o anónimo es uno de los grandes desafíos en estos tiempos de algoritmos. La dark web da ese privilegio. Y, como toda tecnologia, se puede usar para el bien o para el mal. ¿Es cierto que se consiguen sicarios, drogas, armas y pornografía infantil con solo un par de clicks? Axel Marazzi y Tomás Pérez Vizzón recorren historias de las profundidades de internet. La ilustración, a cargo de Emmanuel Cerino, está realizada en 360 grados.

Junio de 2012, Capital Federal. Santiago abrió la laptop, entró a una página, se logueó con usuario y contraseña y pidió dos planchas de LSD. Dos semanas más tarde, recibió un sobre en su casa. Tenía folletos en holandés y un paquete de figuritas de Disney. Me cagaron, pensó. Abrió el paquete: Pluto, Mickey y el Pato Donald. Puta madre. Las revisó detenidamente. La de Pluto tenía una sorpresa: había un sticker que decía We Are Anonymous (Somos Anonymous). Lo despegó y encontró los cartones de 2×2 de LSD.

Puede parecer una escena sacada de una película de ciencia ficción donde las drogas se venden a través de sitios como Amazon o Mercado Libre, pero no. Esta historia es real. Santiago es Santiago Siri, fundador de Democracy Earth, organización sin fines de lucro que desarrolla tecnologías para crear una democracia global digital y descentralizada, y autor del libro “Hacktivismo, la red y su alcance para revolucionar el poder”. El navegador que abrió en su computadora se llama Tor (The Onion Router), la red a la que ingresó es la dark web y el mercado, que ya no existe, era Silk Road.

The Onion Router, la puerta de entrada

Para poder entrar a la dark web hay que descargar Tor, *un google chrome gratuito* con el que cualquier persona puede navegar de manera anónima haciendo muy complicado que terceros puedan interceptarlo. Cuando alguien abre Tor se conecta

a una serie de nodos distribuidos alrededor de todo el mundo que encriptan la información y aumentan la privacidad del usuario logrando que nadie pueda rastrearlo ni saber lo que está haciendo. De ahí el nombre relacionado a la cebolla, cada capa de la cebolla representa un nodo. Si bien Siri estaba pidiendo dosis de LSD desde su casa en la Argentina, Tor nunca revelaría su ubicación exacta.

La tecnología que le dio vida al navegador Tor se llama Onion Routing y fue desarrollada a mediados de los 90s por el Laboratorio de Investigación Naval de Estados Unidos para que las comunicaciones entre militares fueran seguras.

Crear una red que da la posibilidad de ser anónimo es un recurso que, como todas las tecnologías, puede ser usada para el bien o para el mal. No solo otorga la facultad de evitar el espionaje masivo que hacen gobiernos de todo el mundo, sino también le da la capacidad a muchos criminales para mostrar y vender, por ejemplo, armas.

“Me apena muchisimo que usen mi tecnología para delinquir. Pero creo que eliminarla no arreglaría nada. Los que quieren romper la privacidad tienen muchas maneras para hacerlo. Si eliminámaramos redes como la nuestra, lo que conseguiríamos es que fuera el ciudadano medio el que se quedara sin privacidad”, dijo a El País Nick Mathewson, informático del MIT que junto a Roger Dingledine, Nick Mathewson y Paul Syverson, creó The Tor Project en el 2000.

Las tecnologías para el mal

A Iván Barrera Oro lo levantaron a timbrazos a las 7 de la mañana del sábado 16 de junio de 2016. Un escuadrón de la Policía Federal lo esperaba del otro lado de la puerta para hacer un allanamiento en su casa y llevarse computadoras, discos, pen drives, fotos.

—¿Qué hice?

—Producción y distribución de pornografía infantil.

Aturdido, dejó pasar a los agentes y los miró mientras revisaban su casa y preguntaban por cosas que él no entendía. Le habían iniciado una causa.

Barrera Oro se asesoró y se puso a investigar. En agosto de 2013, una persona

utilizó un nodo de salida de la red TOR para subir pornografía infantil en 4chan, una red de foros creada en 2003 para publicar imágenes de forma anónima. El nodo de salida era de Iván. ¿Eso qué quiere decir? No cualquiera tiene una computadora apta para ser nodo de salida TOR. Son procesadores especiales que permiten iniciar la subida de archivos en modo cebolla. Salen de esa computadora y siguen su camino por las distintas capas hasta que se publica de manera anónima.

La cronología sigue. En 2015, un usuario de 4chan denunció el contenido. Desde la red, pasaron el caso a Missing Children, que lo derivó al Ministerio Público Fiscal. Un año después, la policía golpeaba la puerta de Iván Barrera.

“El proceso judicial fue una locura”, dijo Barrera en una conferencia en la EkoParty 2017, donde, junto a su abogado Rodrigo Iglesias, explicó el caso para un auditorio

experto en seguridad informática.

Durante las pericias tuvo que enseñarles a los funcionarios judiciales cómo proceder en estos caso. Les dio la llave (electrónica) para abrir su computadora y no supieron resolverlo. Tuvo que ir a las oficinas a explicarles cómo descifrar la máquina.

Los obstáculos no fueron solo técnicos: “La primera vez que leí el expediente, el juez decía que yo era efectivamente esa persona y que tenía la pornografía en mi casa porque esa IP era mía. Tuve que explicarle a la justicia qué es una IP, por qué yo no soy una IP, que una IP pueden ser muchas personas, qué es TOR y por qué yo no soy eso”.

“No hay un protocolo nacional para hacer una pericia judicial sobre estos temas”, apuntó Rodrigo Iglesias, abogado e investigador de la UBA en ciencia y tecnología, especialista en derecho informático.

Este tipo de situaciones fueron desalentando a muchas personas a tener nodos de salida en Argentina. En 2013, había 8 nodos de salida TOR en el país. Hoy no queda ninguno.

Argentina: El caso Janco

En 2016 Argentina tuvo el primer fallo judicial por un delito cometido en la Deep Web. El jujeño Miguel Abdón Janco fue condenado a 32 años de prisión por “trata de personas con fines de explotación, para promover, facilitar y comercializar pornografía infantil”.

El 6 de enero de 2014, la División Delitos Tecnológicos de la Policía Federal Argentina recibió información del F.B.I. y de la Policía Australiana sobre un usuario de internet localizado en Argentina que descargaba imágenes y videos con pornografía infantil a través de dos páginas.: IMGSRC.RU, una web radicada en Rusia de imágenes y pornografía infantil, y “The Love Zone” (TLZ), a la que solo se accede vía TOR y que se dedica exclusivamente al intercambio de material pornográfico infantil. Para consumir el contenido, el “aspirante a miembro” debía hacer un aporte inicial de 50 megas de material pedófilo inédito y para mantener la membresía se necesitaba una subida mensual de 40 megas.

The Love Zone fue uno de los principales foros de pedófilos: llegó a contar con más

de 47 mil usuarios. Lo cerraron tras comenzar su actividad en 2010 pero luego volvió a funcionar. Su principal operador, el australiano Shannon Grant McCoole, cayó con 100 mil imágenes y 600 videos en su casa.

En The Love Zone Miguel Abdón Janco era un usuario VIP: había subido la cantidad requerida de imágenes y videos con el usuario “miguelboysnew”. Y a IMGSRC.RU subió una sesión de fotos llamada “a beuty boy 3yo before to…” (algo así como “un hermoso chico de 3 años antes de…”), desde la cuenta migueljujuyarg2013@hotmail.com, cuyo IP de creación es en Jujuy, según se detalla en la sentencia 8398/2014 del Tribunal Oral Federal de Jujuy.

La investigación estableció que Miguel Abdón JANCO se filmaba y se fotografiaba a sí mismo manteniendo relaciones sexuales con dos niños para luego intercambiar ese material con otras personas.

Los mercados negros

Uno de los principales destinos de la dark web son los mercados ilegales. Un inmenso bazar caótico en el que se puede encontrar casi todo lo que está fuera de la ley.

Si bien muchas veces se utiliza de manera indistinta el término dark y deep web es importante determinar que no son lo mismo. La deep web son todas esas páginas a las que un buscador no tiene acceso, pero que están a la vista y alcance de todos. El *home banking*, el *SIU-Guaraní*, la página de *AFIP*, por ejemplo. La dark web es otra cosa: a ella se puede acceder solo con Tor. Si tratás de utilizar Chrome o Firefox para entrar a una página te devolverá un error.

En estos últimos años, los mercados que protegen la identidad de los vendedores y compradores crecieron exponencialmente, pero el que marcó el rumbo fue Silk Road, creado por Ross Ulbricht.

Ulbricht estudió física en la Universidad de Texas en Dallas, Estados Unidos, y manejaba un pequeño negocio virtual de libros y hacía *peer-review* (traducción) en investigaciones científicas. En el 2010 escribió en su cuenta de LinkedIn que estaba creando una simulación económica para darle a la gente una experiencia de cómo sería vivir en un mundo sin el uso sistémico de la fuerza. Ese experimento era Silk Road.

Detrás de la idea fundacional de este mercado negro había una ideología libertaria: Ulbricht consideraba que cualquier persona debería poder acceder a lo que deseara sin la intervención de ningún Estado, siempre y cuando no le hiciera mal a un tercero. En los foros de Silk Road escribía manifiestos de diferentes escuelas económicas que estaban en línea con una libertad absoluta de los derechos individuales, del derecho de hacer con tu cuerpo lo que consideres correcto, de no respetar las ideologías de poderes de turno y que nadie dictamine qué se puede hacer con tu vida.

Hoy Ulbricht, de 33 años, está cumpliendo una condena de cadena perpetua en una cárcel de Nueva York por haber sido quien estuvo detrás del pseudónimo Dread Pirate Roberts. Con ese nombre administraba Silk Road, el mercado ilegal más grande en la historia de la dark web: drogas, documentos y billetes falsos, servicios de hackers, software pirata, malware, licencias de conducir y un largo etcétera. Todo estaba fuera de la ley, pero había reglas. No pornografía infantil, no tarjetas de crédito robadas, no sicarios ni armas de cualquier tipo.

Santiago Siri venía investigando de las monedas virtuales y llegó a Silk Road buscando información sobre bitcoins. “Cuando apareció bitcoin en ciertos circuitos de la web circulaba el rumor de que era una moneda que servía para hacer transacciones anónimas y que había mercados en la dark web donde te podías comprar todo tipo de cosas ilegales. Como estaba en el tema, me llamó la atención y empecé a ver si era real o no. Ahí descubrí algo que se llamaba Silk Road”, comenta.

La primera vez que Siri entró a Silk Road se topó con una página en blanco. Presionó el F5 varias veces, pero el sitio seguía dando el mismo resultado. Tras confirmar que la web a la que había ingresado era la correcta, se le ocurrió chequear el código fuente del sitio (el lenguaje de programación en el que está escrita la página). Ahí, escondido, estaba la dirección *real* a la que tenía que ingresar para poder registrarse en Silk Road.

“Te hacías el usuario donde no ponías tu mail ni nada con lo que pudieran rastrearte más tarde (solo te daban un PIN por si perdías el password para poder recuperarlo) y recién ahí accedías al sitio. Me encontré con uno de los catálogos más bizarros que vi en mi vida”, comentó.

Todo es extraño en los mercados negros de la dark web. “Había uno que vendía por

un bitcoin, US$1 en ese momento (¡hoy está cerca de los 17 mil dólares cada uno!), una guía paso a paso para que Amazon te enviara un *Kindle* gratis a tu casa. En la foto del avatar, el vendedor aparecía con 60 *Kindles* atrás y un árbol de Navidad. También había manuales para hackear cajeros automáticos y antenas para interceptar llamadas de todos los celulares que estaban hasta 100 metros a la redonda", recuerda Siri.

El mercado creado por Ulbricht estuvo online durante 2 años y medio y tenía, según se informó en el juicio, casi un millón de usuarios registrados y un total de transacciones que superó los 1.000 millones de dólares.

Las tecnologías para el bien

No todo en la dark web son mercados ilegales donde venden droga, sicarios y parece reinar la anarquía absoluta. Hay personas que la usan para protegerse. Algunos de los primeros usuarios que tuvieron esta tecnología no fueron criminales, sino disidentes que eran buscados e investigados por gobiernos autoritarios.

Edward Snowden, el informático de la CIA y la NSA a quien Donald Trump acusóde traidor a la Patria porque reveló el proyecto PRISM, con el que Estados Unidos espiaba a todos los usuarios de internet que no estuvieran en su territorio, fue uno de los tantos usuarios que se escondió detrás de la tecnología de Tor y la dark web.

"Sin Tor, las calles de internet se volverían como las calles de una ciudad muy vigilada donde hay cámaras en todos lados. Si tu adversario lo quisiera podría seguir las cintas y ver todo lo que hiciste. Con Tor tenemos espacios privados y vidas privadas en donde podemos decidir con quién relacionarnos sin miedo", dijo Snowden.

Periodistas que están realizando investigaciones contra corporaciones o gobiernos, reporteros que se encuentran en países que censuran la conectividad a internet, whistleblowers que tienen información sensible para publicar o militares que deben proteger sus comunicaciones son solo algunas de las personas que utilizan Tor para poder mantenerse anónimos y, de una manera u otra, proteger sus vidas. Eso es lo que los activistas y desarrolladores pretenden cuando crean este tipo de tecnologías.

“Tor es una herramienta importante para los disidentes en los países que se criminaliza la libertad de expresión online”, declaró a Anfibia Ethan Zuckerman, cofundador de Global Voices, una comunidad internacional de bloggers, periodistas, traductores y activistas dedicados a construir una imagen más inclusiva del mundo. “Lo apoyo por una razón muy simple: la vida de mis colegas depende del software”, agregó.

Las personas comunes y corrientes también usan la dark web

Ross Whitaker conocía la dark web y la había navegado algunas veces por curiosidad. Nunca había tenido la intención de comprar nada hasta que su pareja necesitó medicamentos para un problema de asma.

Jackie necesitaba dos tipos de inhaladores: uno para todos los días y otro para situaciones graves. El precio era demasiado alto y no podían pagarlo. Ambos medicamentos costaban U$S300. En un artículo que publicó en VICE contó que debían elegir entre pagar la luz y comprar los inhaladores.

Un día a Jackie, a quien Ross le había contado sobre la dark web, se le ocurrió la idea de que su marido entrara a uno de estos mercados para ver cuánto costaban los remedios. Salían solo U$S30. El 10% de lo que le costaban el cualquier farmacia de Estados Unidos. Sabían que estaba haciendo algo ilegal, pero al mismo tiempo no tenían otra opción.

“No me sorprendió el precio, ya que sabía que los inhaladores se podían comprar en otros países a muy bajo costo –Jackie había comprado uno en una farmacia en Milán por 4 euros–, pero, ¿cómo podría estar seguro de que el vendedor estaba ofreciendo el medicamento real?”, se preguntó Whitaker.

Después de comprobar que las calificaciones del vendedor eran buenas, decidió

adquirirlo. Días más tarde, le llegó un paquete con la medicación y era el mismo producto que podía conseguir a la vuelta de su casa.

Durante algunos unos meses y hasta que pudieron mejorar su situación económica, Ross compró los medicamentos de Jackie a través de la dark web. “Todo lo que sé es que el sistema de salud está roto en este país y hasta que lo solucionen, tal vez no sea tan malo que existan estos mercados negros”, escribió.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.

Fotografía: Emmanuel Cerino

Fecha de creación
2018/01/11