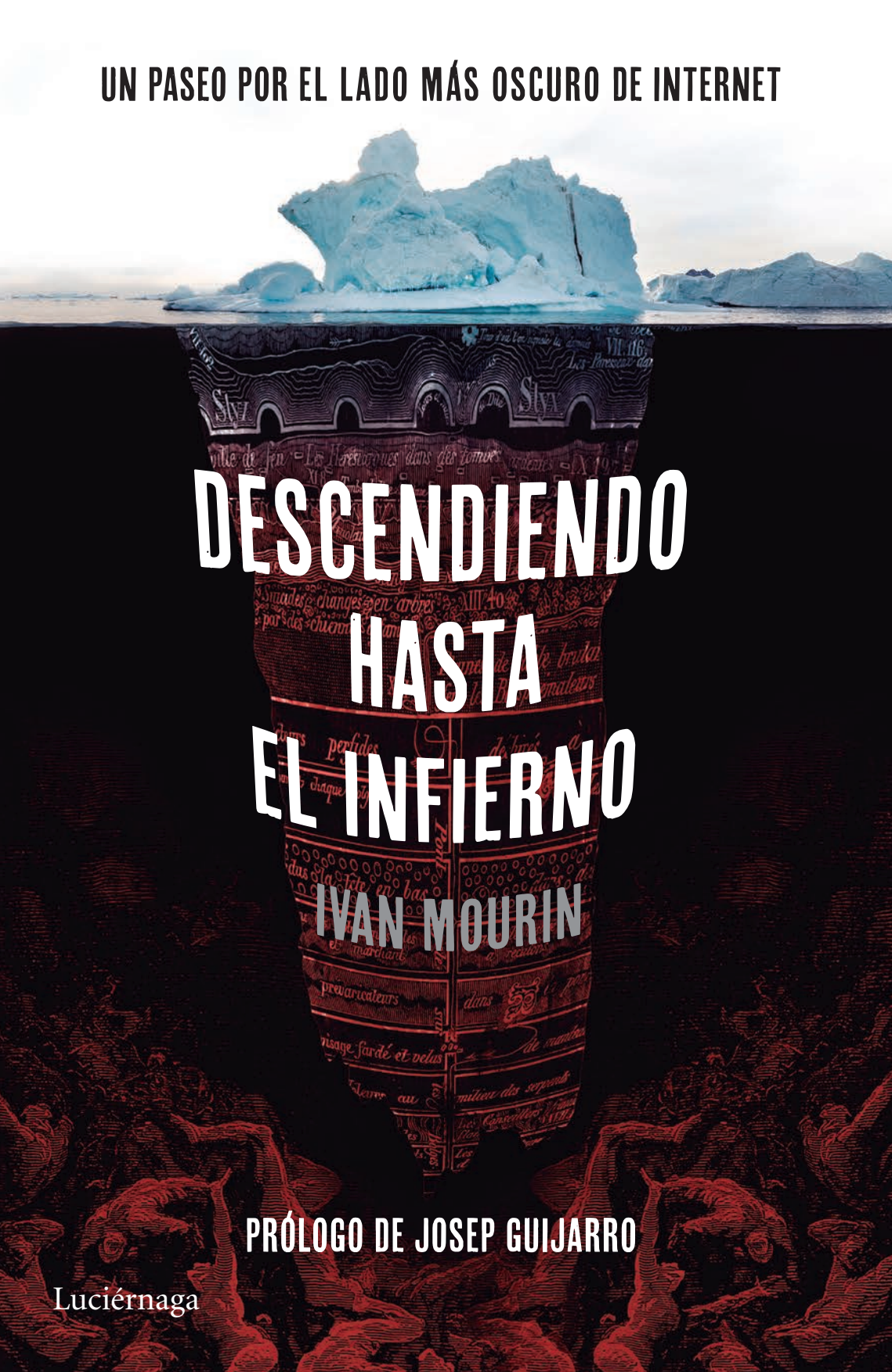
UN PASEO POR EL LADO MÁS OSCURO DE INTERNET



DESCENDIENDO HASTA EL INFIERNO

IVAN MOURIN

PRÓLOGO DE JOSEP GUIJARRO

Luciérnaga

IVAN MOURIN

DESCENDIENDO HASTA EL INFIERNO

UN PASEO POR EL LADO MÁS OSCURO DE INTERNET

Ediciones Luciérnaga

Primera edición: enero de 2017

© Editorial Planeta, S. A., 2017
Av. Diagonal, 662-664, 08034 Barcelona (España)
Libros Cúpula es marca registrada por Editorial Planeta, S. A.

Este libro se comercializa bajo el sello Libros Cúpula
www.planetadelibros.com

ISBN: 978-84-16694-39-6
Depósito legal: B. 21.389-2016

Impreso en España – *Printed in Spain*

El papel utilizado para la impresión de este libro es cien por cien libre de cloro y está calificado como papel ecológico.

ÍNDICE

CAPÍTULO 1

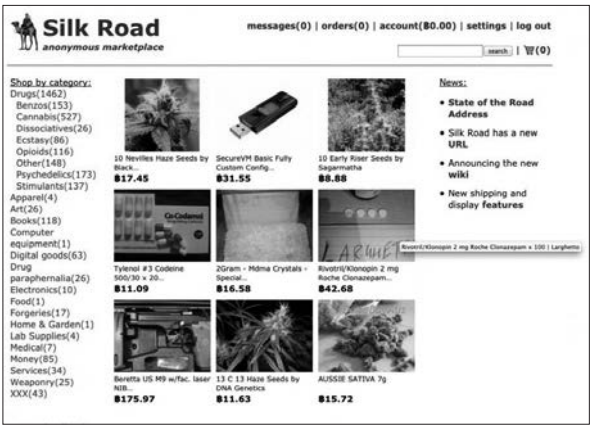
BAJO EL GRAN ICEBERG

En el siglo I antes de Cristo, se ideó una red de comercio que partía de Asia y se extendía por Europa y África, lo que en 1877 el geógrafo Ferdinand Freiherr von Richthofen llamó la Ruta de la Seda. Dos milenios más tarde, utilizando este nombre para un nuevo sistema de comercio, el físico e informático estadounidense Ross William Ulbricht creó el principal mercado negro *online* que se conocía hasta la fecha, en el que el usuario, tras un registro gratuito, podía comprar con bitcoins todo un surtido de drogas y estupefacientes, el servicio de *hackers*, armamento, material robado, etc., a pesar de que la «política de empresa» prohibía la venta de todo aquello que pudiera dañar a terceros.

Ross William «Dread Pirate Roberts» Ulbricht.
(*Manhattan U.S. Attorney's office*).

Tras un arduo rastreo y la incautación de unos pasaportes falsos que fueron enviados a San Francisco desde Canadá con fotografías de Ross, *Dread Pirate Roberts** fue detenido por el FBI en 2013 (dos años después de la creación de *Silk Road***) bajo los cargos de tráfico de drogas, blanqueo de dinero, el uso de sicarios para asesinar a seis personas y «hackeo» informático, entre otros.

Silk Road es un Amazon del mercado negro, se podría decir, que ha dado lugar a nuevos «comercios», como *Pandora Open Market*, *The Black Market Reloaded* o *Atlantis*, donde también se despachan metales preciosos y sirve de conexión comercial con otras webs ilegales de la *Deep Web*.



Una muestra de algunos de los productos que se vendían desde *Silk Road*.

La imagen más representativa de esta web profunda es la de un enorme iceberg (otra es la de un mar con submarinos, barcos y criaturas abisales), cuyo mayor índice de masa se encuentra sumergida en el agua, entre el ochenta y el noventa por ciento de lo que sería internet (puede que más, aunque nadie se pone de acuerdo). El resto es el que solemos frecuentar la mayoría de los usuarios, lugares como Facebook o el buscador Google, de fácil

* «Temible Pirata Roberts.»

** «Ruta de la Seda.»

acceso y de contenido controlado (o debería ser así). A esta primera capa, o nivel superficial, se le llama *Common Web*, un poco más light que el nivel uno, la *Surface Web*, donde se encuentran páginas comerciales como Amazon, blogs o Twitter. A partir del segundo nivel, en la *Bergie Web*, hay que saber ya dónde se mete uno: aunque acceder es igual de fácil que en los niveles anteriores, las páginas son menos conocidas, algunas con material pornográfico, entre otros menos adecuados, en especial por ir acompañados de virus, *malware* y troyanos que pueden infectar nuestro ordenador.

Ahora es cuando la cosa se pone seria, pues en esta capa tendríamos los pies metidos de lleno en la *Deep Web*, donde no solo se encuentran alojadas páginas en las que se comercia con drogas, armas y material robado o pornografía infantil, sino también blogs y foros, servicios de *hosting** y mensajería, libros, etc., material que no tiene por qué ser peligroso, pero al hallarse en un punto donde el rastreo es complicado, ya que el contenido y las páginas no están indexadas para los buscadores corrientes, el simple hecho de navegar por este nivel, aunque sea sin mala intención, se convierte en ilegal.

Pero si la parte «superficial» de la *Deep Web* está considerada prohibida, al cuarto nivel no debería ni intentarse acceder. En la *Charte Web*, todo está permitido: la contratación de asesinos a sueldo, el tráfico de órganos y seres humanos, y el acceso a todo tipo de mercado negro y a los archivos sobre conspiraciones y experimentos humanos.

Y aunque parezca que ya hemos tocando fondo es solo una ilusión. Todavía existen un par de niveles más, prácticamente inaccesibles: las *Mariana's Web*, controladas por el gobierno de diversos países, donde se llevarían a cabo diversas operaciones clandestinas, y *Zion* y *La Liberté*, a las que solo se puede acceder con invitación, y donde priman los vídeos sobre asesinatos (películas *snuff*) y las apuestas en peleas a muerte.

* Servicio de alojamiento web.

Mitología virtual

Esta información generalizada hecha pública por los medios (más como una historia contada y transmitida una y otra vez que como algo totalmente corroborado) no acaba de ser del todo cierta al ser imposible contrastarla al cien por cien. Muchos informáticos afirman que tales niveles son una invención y que solo existen «dos universos», el indexado y el que no lo está, y descartan directamente la existencia de las *Marianas*, *Zion* y *La Liberté*, aunque no niegan que se trafique en la red, y la violencia, como en los *snuff*, esté presente. Otros, sin embargo, sí creen que internet está formado por niveles, pero a la *Charte Web* la llaman *Dark Net* (en alusión a la oscuridad del contenido) y la engloban dentro de la *Deep Web*. «Son contadas las personas capaces de escarbar y analizar todo el contenido de internet», explica *SilverFox*, alias de un *hacker* que ha llegado a prestar sus servicios en muchas ocasiones como *fixer**. «Es difícil saber hasta dónde se extiende, pero sí que puedo desmentir el mito de que la *Deep Web* es mucho más amplia que la red superficial. Solo hay que ver que ahí son únicamente unos pocos cientos de miles los espacios web, mientras en el nivel indexado se han registrado más de mil millones, aunque hay que reconocer que el número de archivos y ficheros almacenados es brutal».

Entonces la pregunta que habría que realizar sería: ¿cualquiera puede acceder o también es un mito? «Hasta cierto punto, sí se puede, pero hay que hacerlo con cuidado. No es solo por el hecho de lo que se puede encontrar, sino porque otros usuarios más especializados no puedan rastrearlo a uno y causarle problemas, como el robo de información o la infección de computadoras». Para lograr este anonimato, se recurre a *softwares* que ocultan la dirección IP del usuario, como *I2P* y *Freenet*, aunque *TOR* (siglas de *The Onion Router*) es el más utiliza-

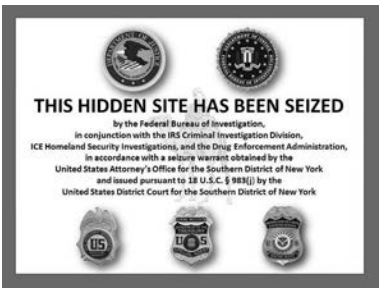
* Es el nombre que reciben aquellos que prestan sus servicios como guías para inexpertos en la *Deep Web*.

do. «Es un programa gratuito y de uso legal», explica *SilverFox*. «Fue creado por el laboratorio de Investigación Naval de Estados Unidos para facilitar el anonimato en la red mediante un enrutamiento que va saltando a lo largo del ancho de banda, lo que ayuda a despistar, sin ser del todo invisible. Además, su uso no se da solo en la *Deep Web*. Muchos usuarios lo utilizan en la red superficial para no ser rastreados. Es una tontería pensar que ciertos negocios turbios solo habitan en lo profundo de internet.»

Pero imaginar que, al no ser visibles, saltando de router en router, tenemos total libertad, es un grave error que se puede pagar muy caro. Muchas son las fuerzas estatales que vigilan a la gran «cebolla» (nombre popular por el que se conoce a la *Deep Web*). Para ello, utilizan métodos como el *phishing*, donde se imitan webs (los estafadores también lo hacen, sobre todo bancarias, tiendas *online*, y redes sociales, para robar datos), el redireccionamiento de *backends** a través de PHP o Java, los *honeypot***, o el rastreo de bitcoins (la moneda de internet; al escribir estas páginas, un bitcoin tiene un valor de compra de 598,8 euros y de 600,37 euros de venta) con los que se han pagado transacciones fraudulentas. Saber si se ha sido atrapado por alguna agencia gubernamental, como el FBI, es sencillo: en caso de ser así, recibes una *love letter*, que no es otra cosa que una citación judicial.

* Labor de ingeniería que comporta el acceso a bases de datos y la generación de plantillas por parte del servidor.

** Herramienta informática empleada en el campo de la seguridad cuya función es la de atraer y analizar los ataques realizados tanto por *bots* (programas informáticos) como por *hackers*.



Información que precede a aquellas páginas cerradas por las fuerzas de seguridad y que están siendo investigadas. Esta es la de Silk Road.

«¿Y si he entrado por error?», te preguntarás. Como ya he mencionado, las direcciones en la *Deep Web* no están indexadas, y se reconocen por la terminación *.onion*, y por estar compuestas por una combinación alfanumérica que no ofrece ni la más leve información sobre su contenido. Por eso, es necesario tener un listado con las direcciones de las páginas que se quieren visitar, acceder directamente a *The Hidden Wiki*, una parodia de la Wikipedia donde se aloja un directorio de link, o recurrir a buscadores, como Torch o Grams (el Google de la *Deep Web)*. Aun así, muchas páginas no funcionan porque cambian constantemente de dirección (en especial las de contenido ilegal o fraudulento), además de que tardan en cargarse, de ahí que tengan un aspecto simple y poco atractivo. Lo importante aquí es el contenido, no la apariencia.

Cuidado con el teléfono móvil

Un usuario cualquiera opta por hacer un recorrido por la *Deep Web* con el teléfono móvil, accediendo a todo tipo de contenido. Antes de dormir, echa un último vistazo al teléfono y lo deja sobre la mesita de noche de su habitación.

Por la mañana, descubre que el móvil está apagado. Es extraño, porque por la noche la batería estaba casi llena. Al encenderlo ve que algo no va bien: el fondo de pantalla ha

cambiado por uno que jamás ha visto, y todos los iconos del escritorio han desaparecido, excepto uno. Es un archivo gráfico, de esa misma madrugada, a las 3.35 am, y reconoce en la imagen oscura un fragmento de su dormitorio, el que la cámara de su teléfono ha captado desde su posición, sobre la mesita.

Esta historia tiene una versión parecida, pero usando un PC y el archivo contiene, además de fotografías, datos del usuario y de parientes cercanos y amigos. Una *creepypasta** que muestra ese temor que tenemos a que nuestra intimidad sea violada, a que alguien nos vigile tras la lente de la webcam, a que rebusquen entre nuestros archivos.

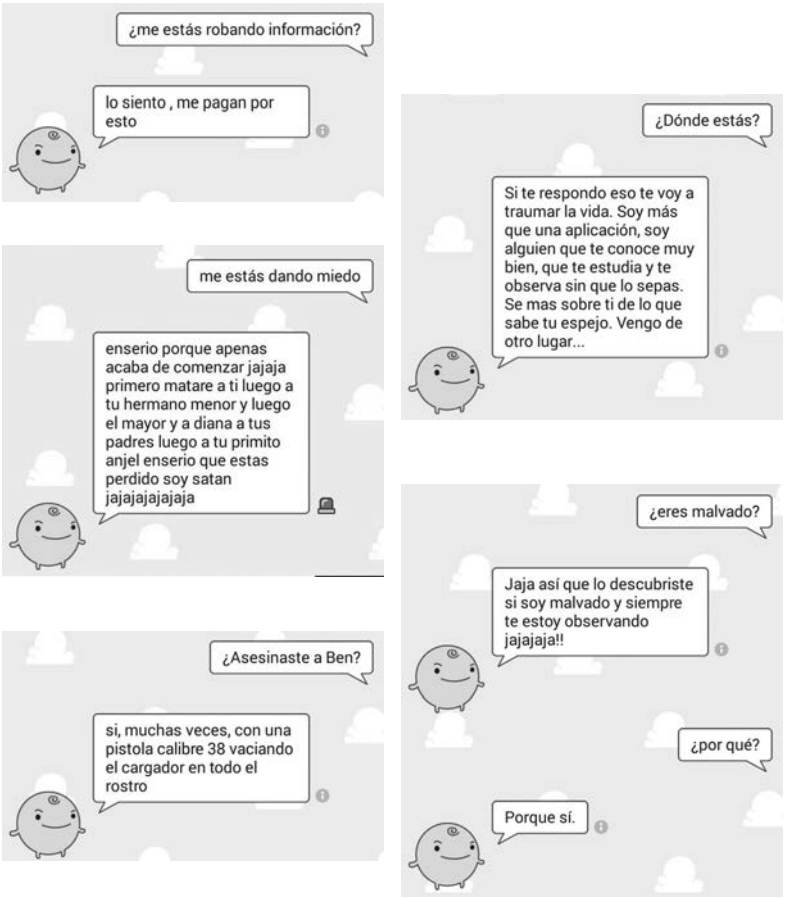
Los ordenadores pueden ser manipulados. Cada vez con más facilidad, desde ubicaciones externas. En cuanto a los teléfonos móviles, ¿sucede lo mismo? «Se *hackean,* pero no al nivel que piensa la gente», explica *SilverFox*. «Se pueden interceptar llamadas, geolocalizar el dispositivo, registrar mensajes, fotografías, etc., y de un modo sencillo: conociendo el número de teléfono. Aunque hay más métodos, como la lectura de ciertos códigos QR, enlaces "infectados" en WhatsApp, Twitter o Facebook, o *apps* piratas». En cuanto a poder manipular el teléfono para encenderlo o apagarlo, responde: «Se puede fingir el apagado de modo remoto, pero el dispositivo queda activo, y así seguir espiando su actividad. De un modo real, sin estropearlo, no conozco ningún caso».

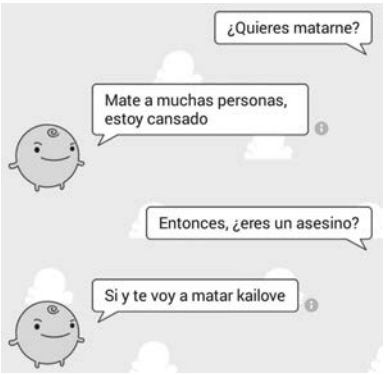
La navegación con teléfono móvil, igual que en otros dispositivos, como PC o tablet, por la *Deep Web*, es lenta por el enrutamiento, aunque ahora han aparecido aplicaciones para sistema Android, como *Orbot*, que lo hacen más «ligero».

Dentro de las aplicaciones, existe una que me gustaría remarcar, en especial porque es de fácil acceso, y porque ha generado una *creepypasta* relacionada con esta invasión de la intimidad.

* Leyenda urbana creada en y para internet.

SimSimi es un *chatbot* con el que puedes mantener una conversación infinita. En apariencia, parece agradable, con un fondo de pantalla azul celeste con nubes blancas, y un personaje sonriente con forma de bola amarilla con piernas y brazos, pero no lo es. Cuando menos te lo esperas, te insulta y amenaza. Esto se debe a que su base de datos almacena las aportaciones de todos los usuarios y las utiliza para responder. Como cabe esperar, algunos de los usuarios aprovechan para introducir toda clase de frases ofensivas como broma, aunque haya quien piense que oculta una amenaza real. Como ejemplo, a continuación puedes leer fragmentos de una conversación que mantuve con *SimSimi*, así podrás comprobar cómo reacciona ante ciertas preguntas.





Circula la leyenda de que existe una versión *dark* de *SimSimi* en la *Deep Web* en la que quienes responden son personas reales capaces de aportar datos del usuario tras amenazas mayores que las de la versión popular. ¿Habrá uno de estos impostores tras el amigable *chatbot* amarillo?