Paakat: Revista de Tecnología y Sociedad
e-ISSN: 2007-3607
Universidad de Guadalajara
Sistema de Universidad Virtual
México
suv.paakat@redudg.udg.mx

Año 10, número 18, marzo-agosto 2020

Recensión
Internet negro. El lado oscuro de la red

Patricia Vargas Portillo*
http://orcid.org/0000-0002-0226-3053
ESIC Business & Marketing School

Obra reseñada: Peré Cervantes y Oliver Tauste. *Internet negro. El lado oscuro de la red*
Ediciones Martínez Roca, Madrid, España, 2016, 248 pp.

[Recibido 08/10/2019. Aceptado para su publicación 29/01/2020]
DOI: http://dx.doi.org/10.32870/Pk.a10n18.465

Cuando en un dispositivo electrónico (computadora, *smartphone*, *tablet*, entre otros) tecleamos las habituales siglas www y, a continuación, la dirección de una página web, accedemos en cuestión segundos a toda la información que, sin la revolución de la tecnología, nos llevaría días, semanas o meses encontrar. No cabe duda que internet nos ha hecho la vida más cómoda y accesible al cambiar de manera abrupta las formas de interacción de la existencia cotidiana pero, de manera simultánea, también nos ha expuesto a riesgos que hace solo algunas décadas eran plenamente inimaginables. De nuevo, en el ámbito que comentamos, al ser testigos y protagonistas, la realidad supera a la ficción.

Como es conocido por todos, la red de redes fue un sistema de comunicaciones diseñado por la industria de la defensa norteamericana. El motivo más significativo de los orígenes de la red radica en factores políticos, pues fue en la década de los sesenta, durante la Guerra Fría, cuando la rivalidad entre las dos grandes potencias, Rusia y Estados Unidos, fomentó la carrera armamentística sin perder de vista el valor que el desarrollo tecnológico tenía en la consecución de los objetivos. En este sentido, los responsables de Defense Advanced Research Projects Agency (DARPA, agencia encargada de proyectos de investigación y desarrollo norteamericana) trataban de encontrar una técnica para conectar sus ordenadores al tener como objetivo promover un sistema de comunicaciones que no pudiera ser bloqueado por una agresión nuclear.

El sistema de interconexión entre todos los ordenadores se verificó por la concurrencia del idioma de conexión y por medio de protocolos. El primer protocolo de control de redes, el Network Control Protocol (NCP), se puso en práctica en 1970 y después de 1983 se implantó el TCP/IP (abreviaturas de Transfer Control Protocol/Internet Protocol, protocolo de control de transferencias/protocolo de Internet), el cual, en la actualidad, funciona en la *World Wide Web* y se ha convertido en un sistema que puede originar daños y perjuicios de diverso alcance.

Los sujetos más temidos en el plano digital, hasta hace relativamente poco tiempo, se englobaban dentro del término de *hackers*. Esta palabra se vincula con los reparadores de cajas telefónicas de Estados Unidos en la década de los cincuenta, cuya principal herramienta de reparación era un golpe brusco al artilugio con fallos, lo que se denominaba *hack*. Anticipadamente, puede decirse que es un informático que recurre a técnicas de penetración no programadas para acceder a un sistema informático con diversos fines. Dentro de estos últimos podemos citar, sin ánimo agotador: satisfacer su curiosidad, superar los filtros preestablecidos, comprobar la vulnerabilidad del sistema para corregir su seguridad; despojar, cambiar, dañar o borrar información.

Las motivaciones de estas acciones, presentadas a modo de ejemplo, también responden a los más variados intereses: ánimo de lucro, posiciones ideológicas anarquistas, ambición de conocimientos, vanidad y divulgación política. Las acciones que hoy se producen, en el ámbito de la *deep web* o Internet profundo, gozan de una amplitud notablemente más significativa que las que se observaron en sus comienzos, a propósito de las acciones maliciosas de los *hackers*. Es necesario apuntar que, junto a los *hackers* de corte malicioso, se abrieron camino los que se calificaron como *hackers* éticos con intenciones más amigables.

El libro, objeto de esta reseña, goza de un total de nueve capítulos que seguidamente se comentarán, de manera somera, resaltando los aspectos más sobresalientes. El primero de ellos, bajo la rúbrica de "Lo que Google ve", se ocupa de los fraudes más comunes en la red. En este sentido, se refiere, entre otros aspectos, al *phishing*, el *pharming*, el *ransomware*, las cartas nigerianas y las falsas *app*. La variedad de estafas es cada vez más amplia y los métodos más sofisticados. Los delincuentes agudizan el ingenio hasta límites inverosímiles. La crisis, lamentablemente, ha facilitado que los más vulnerables o ingenuos caigan en las trampas. El objetivo del *phishing* y del

pharming es robar los fondos que los usuarios tienen en los bancos. El riesgo es demasiado elevado y los peligros cada vez son más numerosos. Todo este tipo de fraudes llega en formato de *spam* (correo electrónico no solicitado) o aplicaciones maliciosas. Este último, como es sabido, es el gran defecto del *marketing* por correo electrónico y el motivo por el que cada vez más empresas prescinden de esta acción por concebirla como invasiva, con escasa vigencia y por confundir una campaña bien estructurada con un envío indiscriminado sin ningún tipo de filtro.

Otras de las estafas más frecuentes eran los "muleros". Estos últimos son intermediarios entre los delincuentes efectivos y los usuarios que han sido víctimas de *phishing*. La forma de reclutar a los muleros, en apariencia legítima, es en virtud de falsas ofertas de trabajo en portales nacionales, pero también en canales de mensajería instantánea o, incluso, *spam*. Otro de los fraudes más habituales de los últimos años es el *phishing car*, que consiste en anuncios de automóviles, generalmente de alta gama, anunciados a muy bajo precio de venta. Una vez abonado el precio, el vendedor jamás aparecerá.

A pesar de los avances tecnológicos en materia de las tarjetas bancarias, el *carding*, o la clonación de tarjetas, continúa. El método de clonación es tan vertiginoso que cualquier persona puede llegar a ser una víctima efectiva sin haber sentido ningún tipo de rareza en los métodos de pago usuales. Los delincuentes consiguen acceder a nuestros datos para transportarlos a una tarjeta en blanco o para efectuar transacciones *online*, para lo que no será necesario el clonado físico. Además, los autores refieren, de manera general, que debemos tener precaución con el denominado *malware*, programas maliciosos que los delincuentes utilizan con diversas finalidades, principalmente para extraer información personal (como números de tarjeta o contraseñas bancarias). Por esto, se debe ser selectivo y cuidadoso con los contenidos a los que se accede.

Debemos reparar, asimismo, en otros fraudes más sofisticados que acontecen en la actualidad. Nos referimos a la práctica denominada *vishing* o fraude telefónico. La suplantación de llamadas telefónicas por parte de las falsas instituciones bancarias es una forma más de operar de los ciberdelincuentes. Mediante el engaño y al repetir, de manera fiel, la imagen auditiva de la entidad financiera, se comunican con los clientes y mencionan un posible cargo no reconocido; al facilitar el nombre completo y algunos números vinculados a las tarjetas, los ciberdelincuentes inquietan y preocupan a las víctimas y, de esta manera, con el factor sorpresa de su lado, realizan un aparente proceso y cancelan la transacción.

El capítulo segundo se dedica a las estafas de las que pueden ser objeto los menores de edad. Nos referimos, entre otras acciones, al ciberacoso. Según datos de la Organización Mundial de la Salud (OMS), España es uno de los países con mayor índice de *ciberbullying*. La Fundación Save the Children, como resultado de una encuesta efectuada a más de 21 000 niños españoles, confirmó que la mitad de ellos señaló haber realizado ciberacoso y un número muy significativo reconoció no saber los motivos por lo que lo hizo. Ahora bien, debemos tener en consideración que este tipo de prácticas se han extrapolado, como bien apuntan los autores de la obra, a los profesores que son objeto de humillaciones por parte de los alumnos que graban estas acciones. Estas conductas se denominan *ciberbaiting*. La

falta de educación y valores en este tipo de acciones es una constante. Si bien los menores se lo toman como una burla o un desafío para ver quién humilla más al profesor, el *ciberbaiting* comporta violaciones graves y sancionables contra el honor, ofensas, amenazas y agresiones. Todas estas acciones representan delitos tipificados en el código penal.

Los menores pueden sufrir otro tipo de acciones frente a las cuales deben protegerse de manera amplia, como el *grooming*, el *sexting* y, en menor medida, el *hacking* o robo de contraseñas personales. Para evitar este tipo de actuaciones, los padres o tutores deben extremar las medidas de vigilancia. Con carácter complementario, cabe instalar filtros de control parental, como Safesearch. La falta de bases morales en el futuro adulto genera serios problemas vinculados con las prácticas que acabamos de enunciar.

El tercer capítulo se ocupa de las novedosas formas de la violencia de género. La violencia acometida contra el género femenino, en muchos casos adolescentes, es un problema muy grave que ha encontrado un nuevo escenario en la red y nuevas formas para su desarrollo. La victimización de las mujeres en el escenario electrónico cobra especial preeminencia inducida por dos características añadidas que presenta la propia red; en primer lugar, se trata de la facilidad para causar perjuicios, auxiliada por un alto nivel de impunidad y los problemas para amparar la privacidad; en segundo lugar, el contacto indisoluble con la víctima que el agresor puede ostentar, de forma específica, a través de los teléfonos inteligentes, las redes sociales y las aplicaciones de diverso alcance.

Otro de los capítulos se dedica a la tercera edad en la red. Como su rúbrica revela, los más analógicos, son, del mismo modo, los más vulnerables. Internet, sin las cautelas necesarias, puede ser un lugar inhóspito para los adultos mayores. Entre los riesgos más habituales para los usuarios de internet de mayor edad, podemos citar: interactuar con sitios web o correos electrónicos maliciosos con fines ilícitos; compartir, sin ser consciente, fotos o videos con delincuentes; violación de la privacidad sin que se den cuenta; y la más habitual: ser víctimas de estafas de diverso alcance. Existen empresas punteras en materia de seguridad informática que realizan actividades de formación en este tema. McAfee, que se integra en Intel Security, lanzó su programa Online Safety for Silver Surfers (seguridad en línea para internautas mayores). Se trata de una iniciativa gratuita donde los empleados de McAfee e Intel forman a las personas mayores y les enseñan de qué manera pueden navegar por internet en forma segura, salvaguardar sus datos y los dispositivos desde donde acceden.

El *hacking* es tema principal en el capítulo siguiente. Aunque generalmente el *hacking*, como se apuntó, se relaciona con un movimiento peyorativo al arrastrar connotaciones ilícitas, existe una figura que debe considerarse. Nos referimos al *hacker* ético, quien se dedica a acceder un sistema para determinar sus potenciales vulnerabilidades, lo que, a su vez, previene la infiltración de *hackers* con fines ilícitos. Son expertos en acceder a sistemas informáticos y de *software* para evaluar, vigorizar y optimizar la seguridad.

Otro de los capítulos se titula "Proteger la empresa en la red" y se refiere a los ataques susceptibles de ser padecidos por las pequeñas y medianas empresas en la

actualidad. Aunque no existen estadísticas relativas al número de delitos que sufren estas empresas, los investigadores indican que los ataques informáticos a las *pymes* se incrementan al mismo ritmo que lo hace la delincuencia en internet: aproximadamente un 30% anual sin incluir la cifra negra (que alude a lo que no se denuncia, cuyos datos concretos son difícilmente cuantificables). La mayor parte de las pequeñas y medianas empresas no pueden asumir el esfuerzo económico que una gran empresa efectúa para resguardar su infraestructura de los servidores. Los ciberdelincuentes optan por cometer infracciones de menor cuantía que un único gran golpe. Asimismo, debe manifestarse que la mayor amenaza para las pymes son los ciberataques como el *ransomware*.

Con buen criterio, en el libro también se estudian las tecnoadicciones o las adicciones a determinados dispositivos electrónicos, que cada vez son más frecuentes y más intensas. El fenómeno al que aludimos incluye todas las formas de abuso de las tecnologías de la información y la comunicación (TIC), las cuales se encuentran comúnmente vinculadas con la adicción extrema a la red o a los teléfonos inteligentes (lo que incluye los videojuegos en la red). Como la realidad pone de manifiesto, cada vez somos más dependientes de estos dispositivos. La necesidad de estar interconectado de forma permanente es una de las señales que presentan los sujetos que sufren estos novedosos trastornos. En realidad, es una relación de dependencia que está vinculada con la ansiedad que suscita no tener WiFi, datos de navegación o batería en los terminales electrónicos.

Otro de los capítulos se dedica, en sentido amplio, al lado oscuro de la red y se titula "Lo que Google no ve". La *deep web* es accesible a través de la red TOR. Casi siempre los medios de comunicación hablan de la *deep web* para relacionarla con las actividades delictivas que se realizan en los fondos infranqueables de la red y muy pocas veces explican qué es. Aproximadamente el 90% del contenido de Internet no es accesible mediante los buscadores. Si se nos permite el símil, es como un iceberg: solo es visible una mínima parte. Se trata de una parte de la *deep web*, que engloba toda la información a la que no puede accederse públicamente. Pueden ser simplemente sitios web convencionales preservados por un *paywall* (que podría traducirse como muro de pago), pero también archivos almacenados en Dropbox, correos depositados en los servidores de un proveedor y todas las páginas que se crean durante pequeños lapsos de tiempo, por ejemplo, cuando se accede a un buscador de viajes y se exhibe el contenido.

Si la *deep web* es, como hemos apuntado, el 90% de la red, la *dark web* ocuparía, por poner una cifra, solo el 0.1% de ella. Es una fracción de internet oculta a los motores de búsqueda, con direcciones IP encubiertas y accesibles únicamente con un navegador web específico para ello. La *dark web*, por consiguiente, es parte inseparable de la *deep web*. La *dark web* representa el contenido que se puede hallar en distintas *darknets*, que son cada una de las redes a las que solo es posible acceder con programas específicos. La más conocida es TOR, pero también existen otras como Freenet, I2P y ZeroNet.

Debe precisarse, asimismo, que la *dark web* no es ilícita por sí misma, ya que presenta bastantes sitios web con contenido constructivo. Además, la *dark web* sirve como refugio a los revolucionarios perseguidos en sus respectivos países donde no impera libertad de expresión. El libro se refiere a uno de los casos más populares en este sentido:

el portal Silk Road, un mercado negro al cual solo se podía acceder mediante el navegador TOR y que solo admitía abonos de *bitcoins* (una moneda electrónica que se fundamenta en el anonimato). Los productos que estaban a la venta eran drogas, armas y otro tipo de actividades ilícitas. El éxito que tuvo este portal (con transacciones por un valor superior a los 9,5 millones de *bitcoins*, lo que, a su vez, equivale a 1,200 millones de dólares) ocasionó que las autoridades norteamericanas se dieran cuenta de sus ilícitas actividades.

Su fundador, que recurría al alias de *Dread Pirate Roberts*, fue reconocido como Ross Ulbricht, quien creció en el seno de una familia de clase media y de niño había sido un *boy scout*. Paradójicamente, Ross no era el genio perverso que los medios y las autoridades habían predicho. No se acreditó que *Dread Pirate Roberts* fuera una sola persona, ya que el sistema de anonimato dejó bastantes aspectos en blanco. *Dread Pirate Roberts* manifestó en una entrevista con Forbes que no era el creador de Silk Road. En este sentido, se manifestó que este nombre de usuario constituía un cargo que pasaría de persona a persona en el avance del sitio web. Fue juzgado y condenado a cadena perpetua. Existen muchas particularidades de este caso que podrían hacernos reflexionar sobre si la pena impuesta fue claramente desproporcionada. Ocuparnos de esta materia, sin duda, superaría los fines de esta reseña.

El libro resulta apasionante. Como su epílogo resalta, vivimos una auténtica revolución gracias a Internet. ¿Alguien puede imaginarse la vida que tenemos sin la red? Sin duda, ha venido para quedarse y evolucionar con nosotros con sus luces y sombras.

Este artículo es de acceso abierto. Los usuarios pueden leer, descargar, distribuir, imprimir y enlazar al texto completo, siempre y cuando sea sin fines de lucro y se cite la fuente.

CÓMO CITAR ESTE ARTÍCULO:

Vargas Portillo, P. (2020). Recensión. Internet negro. El lado oscuro de la red*. Paakat: Revista de Tecnología y Sociedad 10*(18). http://dx.doi.org/10.32870/Pk.a10n18.465

* Es doctora en Ciencias Económicas y Empresariales por la Universidad de Huelva, España. Tiene un diploma en Estudios Avanzados (equivalente a máster) con nota media de sobresaliente por la Universidad de Huelva, España. Ostenta, además, un máster en Administración de Empresas por la Universidad Internacional de Andalucía (España), y máster en Dirección y Gestión de Empresas Turísticas, impartido por la Universidad Francisco de Vitoria, en colaboración con CESAE Business &Tourism School (España).