Internet oscuro, ¿ciudad sin ley?

JAVIER LÓPEZ

Socio de Ecija

ECIJA

Mucha gente piensa que Internet se reduce a las páginas web en las que se puede navegar a través de Google, Yahoo!, Ask, Bing o cualquier otro motor de búsqueda convencional. Sin embargo, esta parte visible (llamada *Surface web* o *Clear web*) supone apenas un 10% de los contenidos alojados en la red, permaneciendo oculto un cibermundo profundo conocido como *Invisible web*, *Hidden web* o *Deep web* (denominación dada por la empresa Bright Planet para contenidos no indexables).

El *Deep web* engloba las webs protegidas, como las páginas de los bancos donde aparecen los datos y las extractos de cada cliente, las que alojan contenidos audiovisuales accesibles mediante pago (Netflix, HBO, Spotify, etc.), las que alojan las cuentas de correo de los usuarios de las webs que prestan servicio de correo electrónico (Gmail, Hotmail, etc.), las páginas de contactos (Meetic, Badoo, etc.) y, en general, cualquier web a la que haya que acceder mediante contraseña y/o que no aparezca en los buscadores. También incluye las páginas dinámicas que se generan al hacer una consulta en la web de una entidad bancaria o en los buscadores de hoteles o vuelos (Kayak, Rastreator, Lastminute, etc.), que son temporales y no se indexan en los buscadores.

Del Deep web al Dark web

En consecuencia, este Internet oculto no sólo no es peligroso ni ilegal, sino que es necesario para cumplir la normativa sobre consumidores, contratación en Internet, privacidad, protección de datos, etc. establecida, entre otras, en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores, la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (GDPR).

Sin embargo, dentro de este internet oculto hay una pequeña parte (se calcula que sobre un 0,1% del total), denominado *Dark web*, que tiene una naturaleza muy distinta, pues en su seno se esconden páginas en las que se pueden realizar actividades ilegales, como visualizar o descargar videos con violencia y sexo extremadamente explícito (asesinatos, violaciones, pornografía infantil, etc.); o que permiten contactar con narcotraficantes, hackers, traficantes de órganos, contrabandistas de armas, sicarios, etc.; o que facilitan el blanqueo de capitales, juego ilegal, compra de documentación falsa, etc.

El acceso a las *darknets* o redes independientes que componen la *Dark web* se hace mediante navegadores específicos como TOR (*The onion router*) o I2P (Invisible Internet Project), que obstaculizan la localización de la identidad de los usuarios al permitir ocultar sus datos y su dirección IP. Esta opacidad viene reforzada por la dificultad para localizar el envío de productos ilegales, que se suelen hacer por correo postal o servicios de mensajería convencional, así como para detectar las transacciones económicas por estas operaciones que, en muchas ocasiones, se hacen mediante criptomonedas (bitcoins), lo que también contribuye al anonimato.

Vigilancia policial

Como en cualquier lugar donde puedan cometerse delitos, algunos de ellos tan graves como los que afectan a la salud pública o la seguridad nacional, el *Dark web* está vigilado por las policías y servicios secretos de la mayoría de los países, que deambulan por él como si fueran un usuario más, con el objetivo de recabar datos y detectar actos criminales. De esta forma, estos ciberdelincuentes (y los que acuden a ellos para obtener material o servicios ilegales) también pueden ser localizados, vigilados y, en ocasiones, detenidos gracias a esta información. Algunos ejemplos de esta actividad policial son las operaciones de incautación de material pedófilo y detención de los responsables de su tráfico ilegal; o la clausura de *Silk Road*, una web anónima de venta de drogas, y la detención de Ross William Ulbricht, quien era su supuesto administrador bajo el alias *Dread Pirate Roberts*.

Aunque el *Dark web* también es usado por algunos usuarios de honestas intenciones con la exclusiva finalidad de proteger su anonimato para salvaguardar su seguridad (por ejemplo, en países donde la libertad de expresión está coartada), lo cierto que es un entorno peligroso en el que proliferan los criminales, por lo que no resulta recomendable navegar en él con carácter general, y aún menos si se carece de suficientes conocimientos técnicos para protegerse de ataques y engaños, pues es un ambiente en el que los hackers acechan a los inexpertos curiosos que se adentran en él y donde es frecuente que se estafe a incautos en busca de oportunidades más o menos legales.