La Red TOR, siglas para The Onion Routing, es una red no privada, sino de privacidad aumentada, que permite la navegación privada, entendiéndose esta como aquella navegación donde se desconoce la identidad real del usuario que navega, y donde sus paquetes están encriptados.

La Red TOR es una dark net, esto quiere decir, una parte de la red no accesible por los medios o navegadores convencionales. La suma de estas Dark Nets conforma la famosa Dark Web.

Cualquier sitio alojado sobre la red TOR suele tener el dominio .onion, y estos dominios normalmente no son accesible mediante la usual forma de escribir su URL en la barra del navegador y entrar, sino que uno es redirigido a estos dominios mediante un enrutamiento.

Como dijimos, TOR significa The Onion Routing. Este nombre viene del modelo de enrutamiento que se utiliza, modelado por la cebolla, por su cantidad de capas. Para llevar un paquete hacia un destinatario en la red TOR, el paquete es sellado en varias capas encriptadas por el emisor. Entonces, este paquete se envía a través de una elección aleatoria de nodos en la red hasta llegar al destinatario final. La trampa está en que cada capa contiene un cifrado, que solo puede ser desencriptado por el nodo actual donde se encuentre ese paquete. El mensaje desencriptado contiene las instrucciones para enviar el paquete al siguiente nodo, y otra vez, un cifrado que solo ese nodo podrá descifrar, y así sucesivamente, hasta que llega al destinatario final, que solo es conocido por el emisor realmente, puesto que ni el número de capas son conocidas a todos.

La desventaja de esto es que el envío de datos se vuelve mucho más lento que de normal, debido a la cantidad de procesamiento necesario para enviar un solo paquete. Por eso, muchas pagínas en la dark web son de texto plano o mucho más básicas que lo que veríamos en el internet convencional. La ventaja, obviamente, es la anonimidad y seguridad que podemos obtener.

Aún así, la red TOR no es infalible, puesto que existen formas de saltarse las medidas de privacidad, si utilizamos nodos comprometidos donde podamos leer los datos (y casos así ya han ocurrido, aunque se han solucionado), o si tuviéramos intervenido el punto final de un envío de datos.

La red TOR es accesible mediante el navegador homónimo, el cual cuenta con varias medidas de seguridad y privacidad, pudiendo elegir entre tres niveles de privacidad, los cuales activan o desactivan funcionalidades del navegador según el nivel. Sin embargo, TOR además viene con recomendaciones, y no seguirlas puede llevar al usuario a exponer su identidad en la red. Este es su otro fallo: Como cualquier herramienta, quien la usa puede romperla.

Cabe destacar que TOR es solo uno de los navegadores de dark net que existen, y que solo se conecta a la red TOR, que está diseñada para el uso público de la gente y es de uso abierto. Existen otros navegadores, más avanzados, que permiten conectarse a otras dark nets o a la totalidad de la dark web, y que no son de conocimiento o uso público.