

# Il lato oscuro della rete

**Internet - Tutti lo citano ma pochi sanno come funziona veramente, cerchiamo di spiegare anche ai «principianti digitali» cosa sia il dark web e quali rischi cela**

/ 16.12.2019  
di Simone Luongo

Chiudi gli occhi e visualizza un enorme iceberg in mezzo allo sconfinato oceano, in una giornata di sole ed in cui vi è calma piatta delle acque. La sua superficie è come una montagna baciata dal sole che riflette un bianco puro e luminoso, con molteplici riflessi cristallini. La tranquillità e la visibilità regnano padrone. Ma oltre quella meraviglia? È noto che l'iceberg emerge per il 10% circa del suo volume, quindi sotto troviamo un'immensa massa di ghiaccio inesplorata, della quale apparentemente non vediamo l'esistenza. Basterebbe immergersi, per qualche metro, e scoprire un'enorme massa di ghiaccio sommersa, in parte ancora raggiunta dai raggi solari, maestosa e di un colore azzurro/blu intenso, non più trasparente come sopra la superficie. Immagina infine di immergerti ancora di più negli abissi, nelle profondità, laddove la luce non arriva, fino a raggiungere la parte più bassa dell'iceberg, la sua base, che appare scura, nera, e di ritrovarti quindi circondato dall'oscurità, dove non sei poi così a tuo agio, sereno, dove la tranquillità non è più garantita, dove non ti senti più al sicuro. Ecco il nostro iceberg paragonato al World Wide Web (il www), dove i miliardi di cristalli di ghiaccio che lo compongono possono essere paragonati alle miliardi di pagine internet del web (stime su [www.worldwidewebsite.com](http://www.worldwidewebsite.com)).

Il world wide web in superficie, vale a dire le pagine che tutti noi possiamo raggiungere per esempio attraverso la semplice ricerca di Google, poiché indicizzate, rappresentano la punta del nostro iceberg. Possiamo così liberamente accedere al sito Wikipedia, alla pagine del nostro e-commerce preferito per acquistare un libro o un oggetto, alle informazioni di cronaca attuali, al sito per viaggi dove prenotare un volo o la prossima vacanza.

Appena sotto la superficie dell'acqua, nella penombra, prende vita il deep web (letteralmente: rete profonda), un'enorme distesa di dati appartenenti a governi e grandi società o istituzioni; i dati sono qui accessibili ad una cerchia di persone che possiede le dovute autorizzazioni e includono dati governativi, rapporti finanziari, informazioni riservate. Il deep web è chiaramente tenuto lontano dai motori di ricerca pubblici ed è protetto mediante potenti firewall, un dispositivo che è in grado di controllare il traffico dati in entrata e in uscita dal sito internet che non vuole essere esposto al pubblico. Tuttavia, queste pagine sono ancora in gran parte connesse ad internet poiché gran parte di queste informazioni costituiscono un ecosistema per molte applicazioni web di superficie.

Più sotto, alla base del nostro iceberg, negli abissi oscuri dove non arriva la luce del sole, prende vita il dark web (letteralmente rete oscura). Nascosto alla nostra vista per vari motivi, quindi irraggiungibile dai motori di ricerca convenzionali; ed è qui che le cose sono messe in ombra e spesso possono divenire pericolose.

Come funziona il dark web?

La rete dark è spesso eseguita su server privati ed è per questa ragione che è di difficile chiusura da parte delle autorità. Per accedervi bisogna affidarsi alla tecnica Onion Routing (TOR), una tecnica che anonimizza le comunicazioni all'interno di una rete di telecomunicazioni; in altre parole, i messaggi vengono criptati (i dati o i segnali sono codificati in modo da risultare incomprensibili a chi non possiede la chiave per decodificarli) e questo garantisce l'anonimato dell'utente dark web. Questo è il motivo che ha portato oggi il dark web ad essere un luogo dove si svolgono numerose attività illegali. Il dominio dei siti internet è qui .onion (invece dei noti .com, .ch, eccetera).

Dopo i primi passi che ci consentono di addentrarci nello sconfinato dark web (in questo articolo non vengono fornite le istruzioni per farlo) è ad esempio possibile digitare i nomi dei principali shop online di TOR, in pratica gli Amazon dell'illegalità. Pochi click e siamo in grado di acquistare droghe di ogni genere; se digitiamo il nome di un'arma da fuoco ecco apparire disponibilità in questo senso. Per spingerci un po' più nel «tecnico» possiamo addirittura acquistare un passaporto falso o il necessario per fabbricarlo, filigrane comprese, oppure una patente di guida, il tutto a prezzi accessibili; ad esempio con meno di 10 franchi possiamo acquistare una carta di credito clonata con i dati del detentore oppure le credenziali di accesso ad un account premium presso il tuo shop online preferito (come Spotify o Amazon). È chiaro che in questi casi siamo di fronte a furti di dati e a veri propri furti d'identità, dove nella pressoché totalità dei casi, la vittima nemmeno è a conoscenza che i suoi dati personali sono stati rubati e si trovano in vendita nel dark web. Chissà pertanto se la Mastercard dell'amico che ci ha raccontato di essere stato vittima di un acquisto con la sua carta di credito, pochi giorni prima non era quotato in un market del dark web.

Il limite non ha limiti, nel vero senso della parola. Sul dark web si possono trovare false lauree universitarie, pedopornografia, animali selvatici protetti; perfino sicari disposti a commettere atti criminali e hackers pronti per pochi soldi a rovinare la reputazione di terze persone violando account di posta elettronica o di social network oppure compromettendo smartphones.

I migliaia di malintenzionati che giornalmente svolgono attività illecite tramite il dark web ben si tutelano al fine di non farsi intercettare dalle autorità. Usano false identità, indirizzi IP nascosti, indirizzi di posta elettronica preposti (fuori discussione ad esempio i noti gmail, hotmail o yahoo), impiegano criptovalute, si fanno recapitare la merce presso un indirizzo non abitato. Questi utilizzatori sono anche ben consapevoli che come esistono i truffatori nel mondo emerso del web, il dark web non ne è da meno, anzi. Data la tipologia di persone frequentatrici del dark web, ovvero personalità propense all'illecito, è inevitabile che merce acquistata non arrivi mai; insomma, chi la fa l'aspetti.

A proposito; nel fare tutto ciò gli avventori di questo mondo sommerso applicano del nastro adesivo sulla lente della web camera, il che è tutto dire sulla pericolosità di questo mondo virtuale. Una sorta di *Hunger Games* (dal noto film) della rete, dove ognuno deve salvaguardarsi dagli altri evitando pericoli quali essere a sua volta crackato, derubato della personalità o di dati personali, di proprie immagini.

Affidatevi ad un esperto del campo, dunque, se per qualche assurda ragione vi venisse voglia di visitare questo lato oscuro della rete.