capisaldi

Dark web: sotto la superficie di Internet

Andrea Carobene
Head of data management, United Risk Management,
<a.carobene@unitedrisk.eu>

Il termine *dark web* indica un insieme di contenuti e servizi della Rete nascosti ai motori di ricerca e che necessitano di appositi programmi per essere raggiunti. Questo spazio virtuale, che garantisce un buon anonimato, può essere usato per comunicare liberamente in contesti politici repressivi, per tutelare la sicurezza dei dati personali, ma anche per svolgere attività illegali. In che cosa consiste esattamente e come funziona? Come si può coniugare la sicurezza pubblica con il rispetto della privacy e delle libertà individuali?

Un ragazzo si impossessa di un laptop, ignorando di averlo sottratto a una persona poco raccomandabile. Esplorandone i contenuti, si trova catapultato, suo malgrado, in un mondo on line di abusi, ricatti e frodi finanziarie, finendo inevitabilmente braccato dal precedente proprietario. È la trama del film *Unfriended: Dark Web* (Stati Uniti 2018), nelle sale dallo scorso marzo. Se la storia è di fantasia, essa però evoca e rispecchia, come sempre accade nel cinema horror, le nostre paure reali, in questo caso l'inquietudine per quanto si muove sotto la superficie del web che navighiamo ogni giorno, confermata periodicamente dalle cronache di reti criminali on line smascherate dagli inquirenti.

In effetti, il web può essere pensato come un oceano diviso in tre grandi zone: il web di superficie, quello profondo e quello oscuro, e come le profondità oceaniche sono a tutt'oggi pressoché inesplorate,

allo stesso modo il web profondo è un territorio sconosciuto ai più, un'ampia zona che sfugge a ogni tentativo di catalogazione e di indicizzazione. Il primo, chiamato anche *clear web* o *surface web* – ossia web in chiaro o di superficie – è formato da tutte le pagine Internet facilmente raggiungibili con i normali motori di ricerca: sono i siti che carichiamo normalmente con i nostri browser. La seconda zona, chiamata *deep web* (letteralmente "web profondo", ma è anche indicata come web nascosto o web invisibile), è rappresentata da pagine che sono normalmente nascoste al pubblico e che non possono essere raggiunte dai motori di ricerca. Probabilmente, ognuno di noi ne conosce e frequenta alcune. Tra queste ad esempio rientrano i siti che richiedono un login e una password per entrare, come le pagine personali di home banking, le e-mail su web, le sezioni a pagamento dei siti di informazione, e così via. In aggiunta, il *deep web* è composto da quelle pagine che sono generate dinamicamente sulla base delle richieste degli utenti, come potrebbe essere la risposta a un'interrogazione per la prenotazione di un viaggio aereo o di un soggiorno in un albergo.

Diverso è il discorso per ciò che riguarda la terza zona del web, indicata col termine *dark*, ossia oscuro. *Deep web* e *dark web* infatti non sono sinonimi. Anche quest'area non è raggiungibile dai motori di ricerca, ma **la sua peculiarità risiede nel fatto che le pagine sono intenzionalmente nascoste, costruite con una modalità particolare che ne garantisce, almeno parzialmente, l'anonimato**, e che possono essere raggiunte solo tramite tecnologie proprie, come ad esempio appositi navigatori. Possiamo dire con ragionevole certezza che la maggior parte di noi utilizza per qualche ragione il *deep web*, mentre ben pochi si avventurano nel *dark web*.

Non è semplice ipotizzare la grandezza rispettiva delle tre aree del web, soprattutto a causa delle caratteristiche proprie delle porzioni *deep* e *dark*. Per quanto riguarda la parte superficiale, ad agosto 2018 i siti indicizzati dai motori di ricerca erano stimati intorno ai 4,4 miliardi[1]. Un numero enorme, se si considera che i secondi della vita lavorativa di un uomo impegnato per 40 anni sono meno di 500 milioni! In pratica, già oggi nessuna persona può navigare l'intero web nel corso della propria vita. Non esiste alcuna stima ufficiale della grandezza del *deep web*, tuttavia la maggior parte degli autori ipotizza che la parte superficiale del web rappresenti solamente il 4% dell'intera mole di dati disponibili in rete (cfr Finklea 2017). In altre parole, siamo di fronte a un vero e proprio iceberg, la cui porzione emersa rappresenta una parte minuscola rispetto a

[1] Dati riportati su <www.worldwidewebsize.com>.

quello che rimane sotto la superficie. Il *dark web* costituisce invece una porzione minima rispetto al *deep web*, e i siti attivi non superano le poche decine di migliaia.

Come funziona il dark web

Per capire come sia possibile misurare il *dark web* occorre prima comprenderne, almeno in minima parte, il funzionamento. **Questa porzione del web è costituita da "reti tra pari" alle quali è possibile accedere solamente con specifici programmi**. Il termine "rete tra pari" si riferisce a un network, in questo caso una rete di server – ossia di computer che interagiscono tra loro fornendo servizi – all'interno del quale nessun nodo, o server, è più importante degli altri. La rete tra pari, dunque, è diversa dai network accentrati, dove alcuni server svolgono un ruolo principale rispetto agli altri dirigendo il traffico, conservando le informazioni e determinando il funzionamento dell'intera rete.

Il *dark web* non ha server centrali e i nodi che lo costituiscono scambiano alla pari le informazioni presenti su questa rete. **Si tratta di sottoreti autonome, gestite da volontari o da specifiche organizzazioni**. Quelle più popolari sono Tor (acronimo di The Onion Router), Freenet, I2P e Riffle. La prima è anche quella maggiormente nota, e si caratterizza per siti il cui indirizzo termina con il suffisso .onion, parola inglese che significa "cipolla". Un sito che termina con .onion non può essere raggiunto da un normale browser, ma necessita dell'apposito navigatore Tor.

La rete Tor, chiamata anche Onionland, è stata costruita per garantire il massimo anonimato possibile ai suoi utilizzatori ed è progettata per nascondere l'indirizzo Ip, ossia l'identificativo del computer utilizzato da chi sta navigando. I pacchetti con i bit delle pagine richieste viaggiano sulla rete senza rivelare appieno l'indirizzo di destinazione, e questo perché tale indirizzo è mascherato da una struttura a strati. Ogni server che riceve un pacchetto legge solamente uno strato, sfogliandolo proprio come se fosse una buccia di una cipolla, e segue le istruzioni ivi riportate per trasmettere il pacchetto al server successivo. Così, di passaggio in passaggio, i dati raggiungono il destinatario senza che alcun server conosca con precisione l'utente che sta navigando su quelle pagine. Altre tecniche, spiegate dettagliatamente sul sito del progetto Tor (<www.torproject.org>), aiutano a preservare ulteriormente la privacy degli utenti del sistema.

Secondo i responsabili del progetto Tor (cfr<https://metrics.torproject.org/hidserv-dir-onions-seen.html>), ad agosto 2018 i siti attivi con domini .onion erano poco più di 100mila. Tuttavia, un'a-

nalisi del 2017, realizzata dal Massachusetts Institute of Technology, ha dimostrato che questa statistica deve essere abbattuta quasi del 90%, in quanto probabilmente nel conteggio sono compresi anche gli utenti di servizi come la chat su Tor o Tor Messenger, che risultano anch'essi identificati con un dominio .onion. Tenendo presente quanto sostenuto in quella ricerca, i veri e propri siti di Onionland non dovrebbero essere più di 15mila (cfr Griffith *et al.* 2017). Stiamo dunque parlando di una percentuale minima rispetto al web in chiaro. In pratica, ogni 250mila siti web in chiaro ve ne è solamente uno appartenente al *dark web*.

Eppure, questa porzione del web ha acquistato, come scrivono i ricercatori del Massachusetts Institute of Technology, una notorietà sinistra: quella di un territorio dove vengono compiute le peggiori nefandezze. L'origine del *dark web* è tuttavia ben diversa da quella di un luogo di delinquenza. Al contrario, **questa rete parallela e il suo browser di riferimento sono nati negli anni '90 come progetto governativo per la sicurezza nazionale nei laboratori di ricerca della marina militare statunitense**, che cercavano di sviluppare un sistema di comunicazione interna, a prova di intercettazione. Nel 2003 il software fu reso disponibile a tutti, come già avvenuto più volte per altre tecnologie di informatica o crittografia sviluppate in ambito militare e successivamente rese di dominio pubblico.

Il progetto The Onion Router

Oggi il programma è gestito dal Progetto Tor, un'organizzazione con sede a Seattle, composta da 35 persone ma che si avvale del contributo di volontari sparsi in tutto il mondo. **L'obiettivo è fornire strumenti utili ai programmatori indipendenti dalle grandi società del settore e garantire la navigazione anonima, per «proteggere la gente dal monitoraggio, dalla sorveglianza e dalla censura»**, come è ribadito sul sito del progetto. Il browser Tor funziona su diversi sistemi operativi e consente la navigazione non solo sui siti .onion, ma sull'intero web in chiaro, mantenendo però intatte le sue funzioni di riservatezza. Una volta installato il navigatore, diventa possibile iniziare a esplorare le pagine .onion del *dark web*, tuttavia la navigazione non è particolarmente semplice, sia per quanto riguarda la velocità, sia per la modalità con la quale sono costruiti gli indirizzi. Le pagine con dominio .onion hanno infatti indirizzi difficilmente interpretabili e memorizzabili, composti da cifre e numeri.

Non esistono motori di ricerca che scandaglino davvero il *dark web*, proprio per la modalità con la quale sono costruiti questi siti. In Rete si trovano delle *directory*, magari suddivise per argomenti, ma che in ogni caso costituiscono una parte minima di Onionland.

Come riportato in un sondaggio tra i navigatori del *dark web*, realizzato nel 2018 dall'Università di Princeton (cfr Winter *et al.* 2018), gli utenti trovano gli indirizzi di riferimento tramite il passaparola, scambiandosi informazioni su alcune bacheche on line come Reddit o ancora utilizzando dei motori di ricerca come DuckDuckGo che forniscono un servizio parziale, ma che possono offrire alcune informazioni.

Per che cosa viene utilizzato il dark web

La cattiva fama del *dark web* è dovuta all'uso illegale che in molti casi ne è stato fatto. Molti siti di questa parte del web si riferiscono infatti ad attività illecite, come il commercio di stupefacenti, la vendita abusiva di armi, la pornografia minorile.

Quattro ricercatori dell'Università spagnola di León hanno provato a effettuare una classificazione dei siti presenti sul *dark web* dividendoli per contenuto (cfr Al Nabki *et al.* 2017). I siti attivi raggiunti dal team spagnolo sono stati 6.831, un valore coerente con altre misurazioni sulla grandezza del *dark web*, almeno per quanto riguarda i domini .onion. Le attività illegali registrate sono state, tra le altre, l'incitamento all'odio, la vendita di documenti contraffatti o di password per accedere a siti, la falsificazione di carte di credito, la vendita di sostanze stupefacenti illegali, il gioco on line, la pornografia, la pedofilia e – in due casi – anche il traffico di esseri umani. **I siti con contenuto certamente illegale sono risultati circa il 27%**. Tra questi spicca il numero di quelli a contenuto pedofilo, circa il 13%, anche se i 914 siti censiti in realtà sono probabilmente meno perché, come notano i ricercatori, vi sono 857 pagine collegate tutte a un unico forum. Le altre pagine dal contenuto lecito si dividono fra siti personali (6%); forum di discussioni, e-mail, news, libri e anche sei siti dedicati alla religione.

La situazione però potrebbe essere peggiore di quanto appare. Uno studio del 2015 di due ricercatori dell'Università di Portsmouth stimava infatti che l'80% del traffico sui siti Tor fosse diretto verso pagine che contengono abusi su persone (cfr Owen e Savage 2015). Parte di questo traffico potrebbe essere realizzata anche dalla polizia, che si connette a questi siti per scopi investigativi, ma si tratta comunque di un dato importante. Va però rilevato che, secondo uno studio realizzato dalla Internet Watch Foundation nel 2014, la maggior parte dei siti con contenuto pedofilo si trova sul web in chiaro o sul *deep web*, e solamente una piccola percentuale, meno dell'1%, appartiene propriamente al *dark web* (cfr Clemmit 2016).

Il mercato nero del dark web

Il commercio svolge un ruolo fondamentale all'interno del *dark web*, in quanto proprio **l'anonimato permette di mettere in vendita oggetti e sostanze illegali**. Spicca l'esempio di Silk Road (Via della seta), un mercato clandestino che è stato chiuso nel 2013 con l'arresto da parte dell'FBI del suo ideatore, Ross William Ulbricht, noto con lo pseudonimo di "Dread Pirate Roberts". Il meccanismo di funzionamento di Silk Road era stato progettato per garantire l'anonimato del venditore e del compratore, assicurando tuttavia che la merce fosse ricevuta e il pagamento realmente effettuato, sul modello di quanto avviene nei negozi on line del web in chiaro. La possibilità di avere una certa garanzia della buona riuscita delle transazioni aveva assicurato a Silk Road lauti guadagni. L'FBI ha calcolato in circa 1,2 miliardi di dollari il fatturato al 2013 di questo mercato clandestino, con un guadagno in commissioni per il suo ideatore di circa 13 milioni di dollari. Si ipotizza che gli acquirenti del sito fossero circa 150mila, serviti da 4mila venditori[2]. Ulbricht è stato condannato al carcere a vita a maggio del 2015, ma nuovi negozi sono nel frattempo sorti, come ad esempio Dream Market o Wall Street Market.

Un esempio particolare di "oggetti" che si possono acquistare scaricandoli da diversi siti sul *dark web* **è rappresentato dai *malware* informatici**, virus da utilizzare per infettare altri computer. È il caso del *ransomware*, ossia un software che cripta i dati del computer vittima e che chiede un riscatto (in inglese *ransom*) per rendere nuovamente accessibili le informazioni. Chi usa questo software ha la possibilità di definire l'entità e le modalità di richiesta del riscatto. Il guadagno viene diviso con l'ideatore del software attraverso un meccanismo inserito nel programma stesso. In tal modo, strumenti atti a compiere reati informatici vengono facilmente messi a disposizione di chiunque. A titolo di esempio, si stima che il *ransomware* CryptoLocker, attivo nel 2013, abbia fruttato al suo ideatore riscatti per tre milioni di dollari (cfr Ward 2014).

Molti dei pagamenti sul *dark web* avvengono con moneta virtuale, ossia con sistemi che sfruttano la *blockchain* (cfr Esposito 2018). In realtà il *bitcoin*, la più nota moneta virtuale, non è la più utilizzata sul *dark web*, in quanto garantisce solo uno pseudoanonimato, poiché ogni transazione è registrata irreversibilmente sulla *blockchain* ed esistono delle tecniche per seguirne i movimenti che

[2] I dati e le informazioni sono contenuti nel documento di accusa della Contea di New York contro Ulbritch (Sealed Complaint County Of Offense: New York, p. 15, <https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf>

consentono potenzialmente di individuare, o almeno di avvicinarsi, ai detentori delle valute informatiche. Si preferisce quindi usare delle monete virtuali che garantiscono un migliore anonimato, come ad esempio Monero, le cui transazioni «non possono essere collegate a un utente particolare o a una identità del mondo reale», come si legge nella home page del sito <www.getmonero.org>.

Il bisogno di tutela della privacy

Tenendo presente quanto è stato detto finora, è possibile fornire una valutazione almeno parziale del fenomeno *dark web*.

Il primo elemento da considerare è che **si tratta di un fenomeno limitato a una porzione minima del web**, pur avendo un grande risalto mediatico. Riteniamo quindi che sia importante averne ben chiara la reale portata, che riguarda oggi una piccola frazione di siti e di utenti del web.

In secondo luogo, è bene portare **l'attenzione al valore della privacy, che costituisce la motivazione originaria** di progetti come Tor. L'esperienza comune è quella che, **a dispetto di ogni regolamentazione, le nostre attività in Rete sono costantemente monitorate a fini almeno pubblicitari**. Se per esempio si compie una ricerca per un albergo in Portogallo su un sito di prenotazione alloggi, è normale che nel proprio computer vengano inserite delle stringhe di codice, chiamate *cookies* – ossia "biscottini" –, che identificano quella richiesta, e che per esempio saranno utilizzate per generare pubblicità mirate su altri siti nel corso della nostra navigazione. La pubblicità, in sintesi, tende a essere mirata sulla base delle nostre esigenze e abitudini di navigazione: una funzionalità presentata come servizio ma che può anche risultare fastidiosa per chi preferirebbe muoversi in maniera maggiormente silenziosa. Lo scandalo di Cambridge Analytica ha poi dimostrato come sia **facile per i colossi del web,** come Facebook, **raccogliere dati personali sugli utenti, realizzando dei veri e propri identikit che possono essere venduti on line** (cfr Greenfield 2018).

La privacy è la prima motivazione per l'utilizzo della rete Tor. Più del 70% degli utenti del *dark web*, secondo il già citato studio dell'Università di Princeton, utilizza infatti tale browser proprio perché garantisce un maggiore anonimato. Il 62% asserisce (erano possibili più risposte) che questa rete offre "maggiore sicurezza", mentre il 47% giustifica la sua scelta con la possibilità di raggiungere contenuti disponibili solamente su questa porzione del web. Il software Tor, come peraltro altri browser[3], offre un buon

[3] Tra questi Epic, Comodo Dragon/Ice Dragon o Freenet.

anonimato anche per chi naviga sul web in chiaro. Rappresenta, quindi, sia una garanzia di maggiore tutela dei dati personali, sia la possibile porta d'ingresso al dark web. **Gli utilizzatori di questi servizi sottolineano l'importanza di barriere contro la censura soprattutto per quei Paesi dove il web e la libertà di pensiero sono limitati**. In reti fortemente centralizzate, come è oggi il web in chiaro, è facile per i Governi non democratici inibire ai propri cittadini l'accesso verso determinati siti, un fenomeno che coinvolge decine di Nazioni. La tecnologia Tor, così come quella di altri strumenti analoghi, permette di aggirare questi vincoli, concedendo una maggiore libertà di navigazione e riducendo nel contempo i rischi per gli utenti di quel Paese.

Tuttavia, come nota l'ex segretario del Dipartimento statunitense per la sicurezza interna Michael Chertoff, «l'anonimato on line è una spada a doppio taglio che deve essere trattata delicatamente» (Chertoff 2017). Se da un lato tutela la privacy e apre spazi di libera comunicazione, per altro verso offre ampi margini d'azione per attività illecite. Nella sua analisi, Chertoff presenta le politiche possibili dei Governi sul *dark web* e conclude con un invito ai Paesi perché collaborino tra loro per stabilire alcune regole. Nel frattempo, il politico statunitense avverte come sia inutile sperare di risolvere il problema da un punto di vista informatico, perché qualunque tentativo di rendere meno anonimo il software Tor finirebbe per dare la spinta a realizzare programmi ancora più anonimi, «azzerando gli sforzi del Governo». Questa analisi mostra che **le problematiche connesse all'uso del *dark web* non possono essere risolte con interventi meramente tecnici o legislativi: le possibilità offerte da tali tecnologie richiedono uno sforzo di riflessione morale e un impegno pedagogico adeguato**. Come scrisse papa Francesco nel suo messaggio per la 50ª Giornata mondiale delle Comunicazioni sociali del 2016, «Non è la tecnologia che determina se la comunicazione è autentica o meno, ma il cuore dell'uomo e la sua capacità di usare bene i mezzi a sua disposizione. [...] La comunicazione, i suoi luoghi e i suoi strumenti hanno comportato un ampliamento di orizzonti per tante persone. Questo è un dono di Dio, ed è anche una grande responsabilità».

È in questa responsabilità che si apre lo **spazio per il discernimento sull'utilizzo di un mezzo come il *dark web*, che è capace di difendere il valore della privacy, ma è anche strumento di atti illegali**. Tale ambivalenza riguarda ogni atto comunicativo dell'uomo, ma la tecnologia la rende più evidente. Ed è per questo che è necessario comprendere questo fenomeno nelle sue diverse dimensioni, evitando giudizi affrettati e manichei, dettati dagli episodi di

cronaca. L'anelito alla libertà, il rispetto dell'individuo e la tensione verso la giustizia sono valori che abitano nel cuore del *dark web* assieme a tanta oscurità, e occorre saper distinguere ciò che vale da ciò che deve essere condannato senza appello.

Al Nabki M.W. *et al.* (2017), «Classifying Illegal Activities on Tor Network Based on Web Textual Contents», in *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics. Valencia, Spain, April 3-7 2013*, *Long Papers*, 1, 35-43, <www.aclweb.org/anthology/E/E17/E17-1004.pdf>.

Bazzel M. (2016), *Hiding from Internet. Eliminating Personal Online Information*, Amazon.

Chertoff M. (2017), «A public policy perspective of the Dark Web», in *Journal of Cyber Policy*, 1, 26-38, <www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1298643>.

Clemmitt M. (2016), *The Dark Web. Does identity-masking technology increase cybercrime?*, CQ Press, <library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500>.

Cunnigham D. – Everton S. – Murphy P. (2015), *Understanding Dark Networks. A Strategic Framework for the Use of Social Network Analysis*, Rowman&Littlefield, Lanham (Maryland, USA).

Esposito M. (2018), «Non solo bitcoin. Le principali applicaizoni della blockchain», in *Aggiornamenti Sociali*, 6-7, 454-462.

Finklea K. (2017), *Dark Web,* Congressional Research Service, marzo, <https://fas.org/sgp/crs/misc/R44101.pdf>.

Papa Francesco (2016), *Messaggio del Santo Padre Francesco per la 50ª giornata mondiale delle comunicazioni sociali. Comunicazione e misericordia: un incontro fecondo*, in <www.vatican.va>.

Greenfield P. (2018), «The Cambridge Analytica files: the story so far», in *The Guardian*, 26 marzo, <www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far>.

Griffith V. – Ratti C. – Yang Xu (2017), *Graph Theoretic Properties of the Darkweb*, 26 aprile, <https://arxiv.org/pdf/1704.07525.pdf>.

Owen G. – Savage N. (2015), «The Tor Dark Net», in *Global Commission on Internet Governance*, <www.cigionline.org/sites/default/files/no20_0.pdf>.

Ward M. (2014), «Cryptolocker victims to get files back for free», in *BBC News*, 6 agosto, <www.bbc.co.uk/news/technology-28661463>.

Winter P. *et al.* (2018), *How Do Tor Users Interact With Onion Services?*, 26 giugno, <arxiv.org/pdf/1806.11278.pdf>.