Wardriving: cos'è? E' legale?

di Commercialista Telematico

Pubblicato il 22 Ottobre 2007

Spesso si sente parlare di Wardriving come condotta più o meno lecita; ma in realtà cosa è il wardriving? (A cura di Avv. Andrea D'Agostini)

Il wardriving non è altro che una ricerca nomadica di reti wireless.

Il che, tradotto in soldoni, significa andare in giro per le città, con computer alla mano (o altri strumenti di ricerca), a cercare reti wireless (WLan).

Ebbene tale tipo di pratica sembra molto diffusa, e se prima si trattava di un'attività di cui si parlava solo nei convegni e tra addetti ai lavori, ora pare che anche la polizia postale abbia rivolto l'attenzione verso i wardriver. Infatti è notizia di qualche tempo fa che una persona a Palermo sia stata denunciata per Wardrinving.

Occorre quindi fare un po' di chiarezza sulla liceità o meno del wardriving.

Innanzi tutto va differenziata l'attività del wardriver che fa una ricerca fine a se stessa, ossia solo per vedere se ci siano reti wireless in un determinato posto e se queste sieano protette o meno (un ricerca fine a se stessa), da quella di ricerca di una rete wireless sprotetta (libera) al fine di utilizzare le risorse di connessione per navigare in rete gratis o fare altre attività.

Nel primo caso, appare chiaro, che la condotta sia penalmente irrilevante, tant'è che il soggetto ricerca alla cieca un access point che poi risulta essere presente o meno.

Il tutto finisce qui con un interrogazione dell'access point che, dal canto suo risponderà, secondo il tipo di rete a cui da accesso.

Tale pratica a volte è del tutto involontaria ed a maggior ragione priva di rilevanza penale: infatti spesso quando si accende un computer portatile che supporti tecnologia wireless questo automaticamente riconosce e avverte l'utente che nella zona ci sono una o più reti wireless e indica se le stesse reti sono libere o protette. In questo caso nessuno soggetto umano interagisce con le reti Wlan e le informazioni che si ricevono sono il risultato di un colloquio fra macchine.

A volte succede che le WLAn aperte quando interrogate da un computer diano addirittura automaticamente un numero IP alla macchina accreditandola così presso di sé.

Anche in questo caso la responsabilità penale dell'utente è nulla.

Diverso è il caso di questi soggetti che una volta trovata una rete, libera o protetta che sia, vi accedano navigando in essa o sfruttandone la banda. In tale ipotesi la responsabilità penale rileva, seppur in diverso modo, a seconda dell'attività posta in essere.

Se la rete è libera (quindi non protetta) il soggetto agente potrà andare incontro a sanzioni, anche gravi, previste dal codice penale. In questo caso, vista la libertà di accesso alla rete, non si potrà configurare il reato di accesso abusivo a sistema informatico o telematico in quanto la rete non prevede misure di sicurezza attive (art. 615 ter cp), mentre a seconda dell'ulteriore attività posta in essere una volta entrato nella rete le ipotesi di reato configurabili possono essere molteplici.

Si va dai reati previsti dagli artt. 617 quater e quinques che riguardano l'intercettazione abusiva di comunicazioni: in questo caso il soggetto che entra nella rete spia quelle che sono le comunicazione del titolare della rete violando così la segretezza della comunicazione stessa, al reato previsto dall'art. 167 del D.Lgs 196/2003, in quanto il wardriver si troverà a trattare dati senza il consenso dell'/gli interessato/i (art 23 D.Lgs 196/2003), passando per la frode informatica (art. 640 ter cp), la sostituzione di persona (art. 494 cp), il danneggiamento di sistemi informatici o telematici di art. 635 bis.

Infatti se una volta entrato, il wardriver si "diverte" a distruggere quello che trova, manda in tilt il sistema, o anche solo parte di esso, incorrerà nella sanzione prevista per il danneggiamento, se invece utilizzerà l'IP della rete per inviare mail o per commettere altri reati sarà responsabile sia della sostituzione di persona sia del reato compiuto a mezzo rete wireless di altri. Un'ulteriore attività si potrebbe

concretizzare anche nell'inserimento di codici malvagi (malware-virus) condotta che rientra nella previsione normativa dell'art. 615 quinques.

Oppure, se utilizza la banda per scaricare o diffondere in rete materiale pedopornografico o comunque materiale protetto dal diritto d'autore, si troverà a rispondere rispondere dei reati disciplinati dagli artt. 600 ter e quater del codice penale e 171 legge sul diritto d'autore.

Altro discorso merita la forzatura della rete, quando questa è protetta (ad esempio con il sistema di cifratura WEP o WPA). In tal caso il wardriver si troverà, per il solo fatto di averla violata superando le misure di sicurezza, nella posizione di chi è entrato abusivamente nel “domicilio informatico” altrui. Si applicherà a tale ipotesi l'art. 615 ter. Una volta entrato, il wardriver potrebbe porre in essere tutte le azione che sono state descritte, per cui si troverebbe a rispondere di tutti i reati consumati.

Insomma la condotta del wardriver va valutata sempre in concreto secondo una scala di infrazioni che vanno dall'accesso abusivo, prima in senso cronologico, alle altre che in base alla volontà dello stesso soggetto saranno poste in essere.

Avv. Andrea D’Agostini

www.Consulentelegaleinformatico.it

www.Consulentelegaleprivacy.it

22 Ottobre 2007