

ISSN 1127-8579

Pubblicato dal 23/10/2015

All'indirizzo <http://www.diritto.it/docs/37471-computer-crime-accesso-abusivo-ad-un-sistema-informatico-e-il-luogo-di-consumazione-del-reato-suprema-corte-di-cassazione-sez-i-penale-sentenza-n-36338-15-depositata-l-8-settembre>

Autore: Iannone Paolo

Computer crime: accesso abusivo ad un sistema informatico e il luogo di consumazione del reato, Suprema Corte di Cassazione, sez. I Penale, sentenza n. 36338/15; depositata l'8 settembre

“Computer crime: accesso abusivo ad un sistema informatico e il luogo di consumazione del reato, Suprema Corte di Cassazione, sez. I Penale, sentenza n. 36338/15; depositata l’8 settembre”

1. Il decisum

La sentenza in commento focalizza la propria attenzione sulla corretta individuazione del luogo di consumazione del reato di accesso abusivo ad un sistema informatico.

La questione approda dinanzi alla Suprema Corte di Cassazione, la quale richiamando una precedente pronuncia delle Sezioni Unite (Cfr. Cass., Sez. Un., n. 17325 del 24 aprile 2015) risolve il conflitto di competenza dei giudici di merito.

2. Il luogo di consumazione del reato

Una delle fattispecie più dibattute nell’ordinamento penale attiene all’accesso abusivo ad un sistema informatico, laddove il reato di cui all’art. 615 ter cod. pen. comprende l’utilizzazione di tecnologie attraverso cui eludere la protezione di dati da un elaboratore elettronico (computer crime).

A riguardo giova rilevare che la condotta posta in essere dall’agente deve presupporre la violazione dei dispositivi di sicurezza, la cui accezione assume valore di manifestazione della volontà del soggetto di accedere, in assenza di autorizzazione, in un sistema informatico o telematico. Tanto chiarito occorre inquadrare la diversa finalità perseguita dall’agente rispetto a quella consentita dalla legge, in quanto determina un elemento imprescindibile nella qualificazione della fattispecie delittuosa.

Ragion per cui il reato di mera condotta si perfeziona con la violazione del c.d. domicilio informatico e, quindi, con l’introduzione abusiva dal proprio elaboratore elettronico.

Ne consegue che, secondo tale impostazione, il comportamento penalmente rilevante del soggetto si realizza dalla propria postazione informatica.

Le superiori considerazioni non si applicano quando la persona avente titolo ad accedere al sistema informatico decida di avvalersi di notizie riservate rilevando a terzi segreti d’ufficio, in quanto tale fattispecie postula altre condotte penalmente rilevanti previste dall’ordinamento e, pertanto, differenti dalla previsione normativa di cui all’art. 615 ter cod. pen. Ciò posto, l’accesso abusivo emerge dall’utilizzazione del sistema informatico per finalità diverse da quelle concesse, pur avendo l’agente titolo per entrare nel software di gestione.

A ben vedere, l’art. 615 ter cod. pen. trova la sua applicazione nell’ambito della mera intrusione non autorizzata e mantenuta contro la volontà del titolare, laddove nel disegno criminoso non vi sia, come unico obiettivo voluto dall’agente, la lesione del diritto alla privacy e la divulgazione di dati riservati.

Ne deriva che, nel caso di specie, il bene-interesse protetto dalla norma è rappresentato dalla violazione del c.d. domicilio informatico accedendo a dati e notizie di pertinenza della sfera giuridica altrui.

In tale prospettiva, la consumazione della fattispecie delittuosa si verifica nel luogo ove avviene l’accesso informatico.

A fondamento di tale ragionamento il reato in questione non concerne la mera effrazione di password o altri sistemi di protezione, poiché la condotta assume rilevanza ai fini della qualificazione del delitto previsto all’art. 615 ter se l’accesso al sistema informatico viene mantenuto contro la volontà del titolare.

Ne consegue che, secondo tale prospettiva, il luogo di consumazione del reato coincide con quello dove l’agente pone in essere la condotta dal proprio elaboratore elettronico eludendo le misure di sicurezza nella procedura di identificazione.

3. Conclusioni

Alla luce di quanto sin qui esposto la sentenza in commento ha il pregio di porre l'attenzione sulla corretta individuazione del luogo di consumazione del delitto di accesso abusivo ad un sistema informatico.

A riguardo giova inquadrare la vicenda in esame nell'ambito dell'intrusione non autorizzata nel flusso di dati informatici disponibili nel cyberspazio della rete internet, laddove le informazioni si trovano nella piena disponibilità dell'utente, la cui visualizzazione risulti reperibile attraverso la digitalizzazione di una password di accesso. Tanto rilevato occorre analizzare il concetto di azione penalmente rilevante con riferimento agli impulsi elettronici scaturiti dal consapevole atto umano dinanzi all'elaboratore informatico. Su tale elemento si fonda la corretta individuazione del luogo di consumazione del reato e, quindi, l'ubicazione del server dove viene posta in essere l'azione funge da rilevatore per la collocazione spaziale dell'intrusione abusiva e circolazione di dati. Ne consegue che il territorio dove si realizza il reato non avviene nella medesima sede del server che controlla gli accessi e conserva le notizie.

A ben vedere, la natura del delitto è rappresentata dall'introduzione non autorizzata e reiterata nel sistema informatico, violando, in particolare, quello spazio virtuale che ospita i dati sul server.

Nel caso di specie viene interpretata la violazione del c.d. domicilio informatico in corrispondenza con l'immissione virtuale in un account altrui da un dispositivo elettronico, ove si instaura un rapporto di collegamento con l'elaboratore informatico. Tale assunto si pone su di una relazione tra l'elusione di protezione al software di gestione e il sistema telematico dal quale avviene l'accesso abusivo. Ciò posto, l'effrazione del sistema di sicurezza si realizza con l'unica condotta umana di natura materiale che presuppone la composizione delle credenziali di autenticazione e, quindi, i dati comunicativi del software rappresentano l'evento successivo del reato. Di conseguenza, l'ingresso non autorizzato eseguito da una postazione computer individua lo spazio fisico in cui la norma viene violata a conferma dell'unicità dell'azione materiale posta in essere dal soggetto.

In tale prospettiva si è orientata la Suprema Corte di Cassazione che ha ritenuto meritevole di attenzione il luogo di accesso della postazione remota dal quale si è realizzata la fattispecie delittuosa, in quanto l'elaborato elettronico utilizzato dall'agente per compiere il delitto non deve essere inteso come elemento passivo della sua condotta, bensì parte integrante del reato in questione.

Dott. Paolo Iannone

• **NORMATIVA DI RIFERIMENTO** •

Art. 615 ter cod. pen.

• **BIBLIOGRAFIA** •

- G. Fiandaca, *Diritto penale, Parte generale*, Bologna;
- F. Mantovani, *Diritto penale, Parte generale*, Padova.