



CAMMINO DIRITTO

Rivista di informazione giuridica
<https://rivista.camminodiritto.it>



SENTENZA CASSAZIONE N. 17325 DEL 26 MARZO 2015: STABILITO IL GIUDICE COMPETENTE IN CASO DI ACCESSO ILLECITO A SISTEMI INFORMATICI

L'accesso ai sistemi informatici altrui sembra poter creare problemi per l'individuazione del giudice competente. La Corte di Cassazione risolve la questione con l'elaborazione di un principio di diritto.

di **Matteo Consiglio**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Publicato, Martedì 12 Maggio 2015

Al giorno d'oggi, nell'era della globalizzazione massiccia e di un mondo che non può più fare a meno della **rete internet**, risulta complessa, per la giurisprudenza, la risoluzione di particolari tematiche tra le quali quella relativa all'individuazione del giudice competente a giudicare quei soggetti che s'introducono abusivamente nei sistemi informatici altrui.

Un'interessante sentenza è quella pronunciata dalle **S.U. della Corte di Cassazione, n. 17325 del 26/03/15**, che regola un **conflitto di competenza**. Il fatto che ne costituisce oggetto vede decorrere il proprio dies a quo dall'esercizio dell'azione penale da parte della Procura della Repubblica di Napoli nei confronti di Michelina Rocco, impiegata della motorizzazione civile di Napoli, e di Giuseppe Schettino per i reati previsti dagli **artt. 81, 110 e 615-ter co. 2 e 3 c.p.** La Procura aveva contestato ai due soggetti l'effettuazione, in concorso tra di loro, di un accesso abusivo nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti con lo scopo di visionare dei dati che esulavano dalle mansioni lavorative della Sig.ra Rocco, interessando, esclusivamente, gli interessi del signor Schettino in qualità di amministratore di un'agenzia di pratiche automobilistiche.

La questione è giunta in Corte di Cassazione al fine risolvere un **conflitto negativo di competenza per territorio** sorto tra il GUP di Napoli e il GUP del Tribunale di Roma. Il primo riteneva che la competenza fosse da individuarsi presso il giudice di Roma, in ragione del fatto che la banca dati della Motorizzazione civile fosse ubicata presso quella del Ministero delle Infrastrutture e dei trasporti in Roma, mentre il secondo riteneva che la competenza appartenesse al giudice del luogo in cui l'operatore aveva agito.

Investite della questione, le S.U. della Corte di Cassazione si sono trovate a dover operare una scelta sulla base di due diverse opzioni che, in buona sostanza, si riflettevano in quelle prospettate dai giudici dichiaratisi incompetenti:

la prima soluzione era quella di radicare la competenza presso il giudice del luogo nel quale il soggetto si era connesso alla rete; la seconda soluzione era quella di incardinare la competenza presso il giudice del luogo ove era collocata la banca dati oggetto d'intrusione. La Corte di Cassazione si era già occupata della questione, con **sentenza n. 40303 del 27/05/2013**, stabilendo che la **competenza** fosse da individuarsi **presso il giudice del luogo in cui era allocato il server**. In tal modo, venne stabilito il principio secondo il quale la fattispecie di **reato si perfezionava nel momento in cui il soggetto agente effettuava l'accesso nel sistema altrui, o vi permaneva, in violazione del domicilio informatico**.

Dall'analisi dell'art. 615-ter c.p. risulta che questa norma, di diritto sostanziale, è stata inserita non a caso nel libro del codice penale che si occupa dell'inviolabilità del

domicilio, in quanto la ratio sottesa è quella di assicurare uno spazio ideale nel quale proteggere i contenuti informatici della persona che ne è titolare. Questo ideale **parallelismo con il domicilio reale** spiega il motivo in virtù del quale la norma è stata inserita nel libro del codice penale che disciplina l'inviolabilità del domicilio.

La Corte, nella decisione in commento, ha sostenuto l'idea secondo la quale al fine di integrare il reato previsto dalla norma penale, **bisogna distinguere le due nozioni di introduzione e di intrattenimento nel sistema informatico**. Per imputare ad un soggetto l'accesso abusivo ad un sistema informatico o telematico risulta necessaria la mera introduzione all'interno di esse senza la necessità che a questa susseguisca il concreto verificarsi di effettive lesioni del diritto alla riservatezza dei dati personali. Per tale motivo, l'eventuale utilizzo di quest'ultimi comporterebbe l'integrazione di una diversa fattispecie di reato.

Oltre a soffermarsi sull'analisi della norma, la Corte ha ragionato anche sulla definizione di sistema informatico accogliendone un'ampia visione al fine di concederne la più vasta tutela. Il giudice di legittimità ha sostenuto che il **c.d. cyberspazio** (la rete internet) comporta una messa in crisi dei tradizionali canoni spazio-temporali di collocazione delle condotte umane, le quali, infatti, si ritengono "delocalizzate".

In virtù di ciò, è stato deciso che, tra le due ipotesi di cui sopra, quella da accogliere fosse la prima, che individua la competenza presso il giudice del luogo in cui il soggetto, o i soggetti nel caso di specie, effettuano l'accesso al server indipendentemente dal luogo in cui, quest'ultimo, sia situato.

La fattispecie di reato viene integrata nel luogo in cui l'operatore materialmente digita la password di accesso al server da violare, realizzando l'accesso alla banca-dati e determinando, così, il momento del superamento delle barriere apposte dal titolare del sistema.

Per queste motivazioni, la Corte di Cassazione ritiene, altresì, rispettato il **principio costituzionale del diritto al giudice naturale precostituito per legge, ex art. 25 Cost.** Difatti, ai sensi di una sentenza della Corte Costituzionale, la **n.168 del 2006**, la "naturalità" assume "un carattere del tutto particolare, giacché la celebrazione di quel processo in quel luogo, risponde ad esigenze di indubbio rilievo, fra le quali, non ultima, va annoverata quella per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati".

Per tale motivo se l'azione si realizza in un certo luogo non v'è ragione per non incardinare la competenza presso il giudice del luogo in cui si è verificato materialmente

il fatto.

La Corte nel disporre la sentenza ha stabilito il principio di diritto secondo il quale: **“Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all’art. 615-ter c.p., è quello nel quale si trova il soggetto che effettua l’introduzione abusiva o vi si mantiene abusivamente”**.

Nel caso di specie, quindi, la competenza è stata individuata presso il GUP del Tribunale di Napoli.
