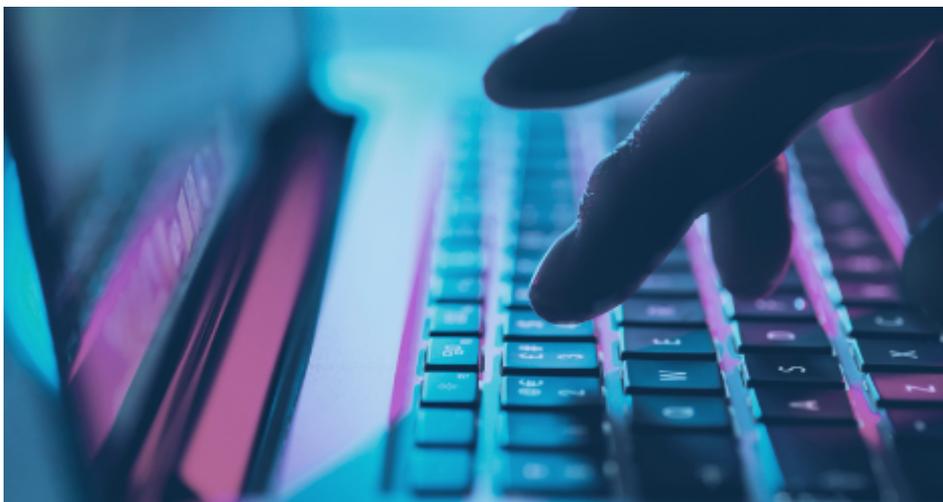


LA CORTE DI CASSAZIONE AMPLIA LA DEFINIZIONE DEL REATO DI ACCESSO ABUSIVO A UN SISTEMA INFORMATICO

01/12/2024

di Gianluca Mariani



Con la sentenza n. **40295 del 31 ottobre 2024**, la Corte di **Cassazione** ha fornito una chiarificazione cruciale sull'applicazione dell'**articolo 615-ter del Codice Penale** italiano. Questa norma, che tutela la riservatezza e l'inviolabilità del "**domicilio digitale**", punisce l'accesso abusivo a un sistema informatico o telematico protetto da misure di sicurezza. La decisione della Corte ha ampliato il concetto di **accesso abusivo**, includendo anche comportamenti interni alle organizzazioni.

Il caso: l'accesso disfunzionale

La vicenda riguardava un direttore di una struttura alberghiera che aveva utilizzato credenziali fornite da una collega per accedere a un database aziendale contenente circa 90.000 schede di clienti. Questo accesso, seppur avvenuto tramite credenziali valide, è stato giudicato abusivo poiché effettuato per scopi estranei al mandato ricevuto.

La Corte d'Appello di Firenze aveva già introdotto il concetto di "**accesso disfunzionale**", ovvero l'uso improprio di credenziali legittime per finalità non autorizzate, confermando la condanna per il reato di accesso abusivo a un sistema informatico.

La decisione della Cassazione

La Corte ha confermato che il reato si configura anche in presenza di un accesso interno, se questo avviene violando le direttive del datore di lavoro o superando i limiti impliciti dettati dall'organizzazione aziendale.

- **Il ruolo delle credenziali personali:** La Corte ha evidenziato che la protezione di un sistema mediante credenziali uniche implica un divieto implicito per altri, anche in posizione gerarchica superiore, di accedere senza autorizzazione.

- **L'accesso non giustificato:** Non è necessario dimostrare un danno concreto o una finalità fraudolenta per configurare il reato. È sufficiente l'accesso non autorizzato a dati protetti.

La prescrizione e le conseguenze civili

Nonostante il reato sia stato dichiarato estinto per prescrizione, le responsabilità civili sono state confermate. L'imputato è stato condannato a risarcire la parte civile, poiché il comportamento è stato giudicato lesivo delle norme civili e delle direttive aziendali.

Implicazioni pratiche e giuridiche

1. Per le aziende:

- La sentenza sottolinea l'importanza di adottare politiche di sicurezza chiare, garantendo che l'accesso ai sistemi sia strettamente regolamentato.
- È cruciale che le direttive aziendali siano formalizzate per evitare comportamenti ambigui.

2. Per i dipendenti:

- Anche chi possiede ruoli apicali deve rispettare le regole aziendali. L'accesso a sistemi informatici protetti senza autorizzazione esplicita può portare a conseguenze penali e civili.
- La giustificazione di un accesso con finalità di controllo o tutela non è sufficiente, se non avallata dall'azienda.

La **sentenza n. 40295 del 2024** rappresenta un importante sviluppo nella giurisprudenza italiana sui **reati informatici**. Essa rafforza la protezione del domicilio digitale, estendendo l'applicazione dell'articolo 615-ter anche agli accessi impropri all'interno delle organizzazioni. Questo verdetto sottolinea la necessità di rispettare le regole aziendali e di adottare misure rigorose per la tutela dei dati.