

## Il reato di accesso abusivo a sistema informatico

**Autore:** Redazione

**In:** Diritto penale

Di seguito un breve disamina relativa al reato di accesso abusivo a sistema informatico ex art. 615-ter c.p.

**Il presente contributo in tema di accesso abusivo a sistema informatico ex art. 615-ter c.p. è tratto da “La responsabilità nei nuovi reati informatici” (A.A. V.V.) a cura di Flaviano Peluso.**

### La natura del reato di accesso abusivo a sistema informatico ex art. 615-ter c.p.

L'accesso abusivo a sistema informatico è il reato p. e p. dall'art. 615-ter c.p. che sancisce: “chiunque abusivamente **si introduce** in un sistema informatico o telematico protetto da misure di sicurezza, **ovvero vi si mantiene** contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione fino a tre anni”.

La norma, posta tra i delitti contro la **inviolabilità del domicilio (art. 614 c.p.)** da cui assorbe la stessa funzione sociale e, sostanzialmente, lo stesso trattamento sanzionatorio, prende in considerazione due condotte: quella dell'accesso non autorizzato, rectius abusivo, ad un sistema informatico o telematico, e quella dell'illecito mantenimento.

La scelta del legislatore di operare questa distinzione appare corretta in quanto esiste la concreta possibilità che **un soggetto acceda, perché autorizzato**, legittimamente all'interno di un sistema ma decida successivamente di trattenersi in maniera abusiva.

Il mantenimento abusivo si configura anche quando il reo utilizzi il sistema **per finalità diverse, o ulteriori**, rispetto a quelle per cui era stato inizialmente autorizzato l'accesso.

Il reato è ritenuto **plurioffensivo**, secondo autorevole dottrina, quando oggetto di offesa e tutela penale sono beni giuridici ed interessi eterogenei, primo fra tutti il **diritto alla riservatezza** e, connesso a questo, quello della **protezione del domicilio informatico**, estensione naturale di quello materiale.

Inoltre, vengono tutelati anche i **diritti di carattere patrimoniale**, come il diritto all'uso del computer per fini economici e produttivi, e gli interessi collettivi, come quelli di carattere militare, sanitari, oppure relativi all'ordine e alla sicurezza pubblica, che potrebbero essere compromessi da intrusioni e

manomissioni non autorizzate.

In realtà il bene giuridico tutelato dalla norma è **essenzialmente uno**: l'inviolabilità del domicilio informatico.

Sia la collocazione della norma (titolo XII, libro I, del codice penale), sia la finalità della stessa (l'articolo non fa alcun riferimento alle informazioni o ai dati custoditi all'interno del sistema) non lasciano dubbi interpretativi sul bene giuridico tutelato, considerando che il reato si verrebbe a configurare anche nel caso in cui il sistema risultasse totalmente privo di dati, così come accade per la violazione di domicilio, che si configura anche nell'eventualità di accesso abusivo in un appartamento vuoto.

**Ti potrebbe interessare anche il seguente articolo: "Il caso Tiziana Cantone, i social network e la web reputation".**

## **Distinzione tra l'accesso abusivo ed il mantenimento.**

La distinzione tra l'accesso abusivo ed il mantenimento assume rilevanza anche con riguardo al tempus commissi delicti. Ed invero, in caso di accesso abusivo si avrà un **reato a consumazione istantanea** che si perfeziona nel momento stesso in cui il reo accede abusivamente al sistema.

Per quanto riguarda il mantenimento è necessario fare una distinzione: nell'eventualità in cui il soggetto agente utilizzi il sistema per finalità ulteriori rispetto a quelle per cui era stato inizialmente autorizzato avremo un reato a consumazione istantanea, mentre nell'eventualità che il reo si trattienga all'interno del sistema, superando così il limite temporale imposto dal titolare, avremo un **reato permanente**, ovvero che si perfeziona nel momento in cui il soggetto agente interrompe la propria condotta criminale.

## **Cosa si intende per "misure di sicurezza"**

Altro elemento saliente della norma è rappresentato dalle "misure di sicurezza". L'accesso, infatti, affinché rientri nella previsione del reato deve essere compiuto **violando le misure difensive** poste dal titolare a difesa del sistema.

Il reato di accesso abusivo a sistema informatico è, pertanto, un reato a forma vincolata, che presuppone l'esistenza di misure di sicurezza per la sua applicabilità.

La giurisprudenza e la dottrina, infatti, ritengono che la fattispecie in esame non richieda una particolare efficacia delle misure di sicurezza adottate a salvaguardia del sistema, ma è necessaria la **volontà del titolare di reprimere qualsiasi irruzione con accorgimenti tecnici, informatici e logici, anche se**

**facilmente aggirabili.**

ne consegue che il reato si perfeziona anche se viene violata una sola misura di sicurezza, non rilevando né il numero né, tantomeno, l'efficacia delle difese adottate dal titolare.

Dal punto di vista prettamente tecnico, le misure di sicurezza possono essere divise in due grandi categorie: **misure di sicurezza digitali e misure di sicurezza non digitali**. Le prime si suddividono a loro volta tra quelle software (password, firewall) ed hardware (firma digitale o riconoscimento biometrico). Le seconde vengono utilizzate per proteggere il sistema informatico o telematico con riguardo alla loro materialità (cassaforte, armadietto).

Le misure di sicurezza di cui all'art. 615-ter c.p. sono quelle riferibili al sistema, e non ai luoghi in cui questo viene custodito. Di conseguenza, anche ai fini del tentativo di reato, le misure di sicurezza che dovranno risultare violate saranno quelle di tipo software e/o hardware.

## Elemento soggettivo

L'elemento soggettivo è rappresentato dal **dolo generico**, ovvero il soggetto agente deve avere la coscienza e la volontà di accedere ad un sistema informatico o telematico provvisto di misure di sicurezza, a nulla rilevando sia il muovente che le finalità del reo.

## Circostanze aggravanti

Le circostanze aggravanti della fattispecie in esame riguardano la condotta, ossia **se il reo è armato o agisce con violenza su persone o cose, la natura del sistema informatico o telematico, sistemi militari o riguardanti l'ordine pubblico, la sanità, o comunque di interesse pubblico**, le conseguenze della condotta, ossia se il sistema venga danneggiato o distrutto, e lo status personale del reo, ovvero se commesso da pubblico ufficiale o da incaricato di pubblico servizio con abuso di poteri, da chi esercita la professione di investigatore privato o con abuso della qualità di operatore di sistema.

Con riguardo alle circostanze aggravanti, nello specifico allo status personale del reo in veste di pubblico ufficiale o di incaricato di pubblico servizio, risulta opportuno segnalare il caso affrontato dalle sezioni unite penali della Suprema Corte di Cassazione con la sentenza n. 41210/2017.

**Il presente contributo in tema di accesso abusivo a sistema informatico ex art. 615-ter c.p. è tratto da "La responsabilità nei nuovi reati informatici" (A.A. V.V.) a cura di Flaviano Peluso.**

<https://www.diritto.it/il-reato-di-accesso-abusivo-a-sistema-informatico/>