CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

PER LA CASSAZIONE IL SUPERIORE CHE ACCEDE CON LE CREDENZIALI DEL SUBORDINATO COMMETTE ACCESSO ABUSIVO A SISTEMA INFORMATICO

La Corte di cassazione con sentenza del 31/10/2024, n. 40295, il dipendente gerarchicamente sovraordinata commette il delitto di accesso abusivo a sistema informatico se si fa rivelare dal sottoposto le credenziali di accesso al sistema per farvi accesso.

di **Andrea Diamante**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Mercoledì 27 Agosto 2025

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The Supreme Court with sentence of 31th October 2024, n. 40294, established that the employee hierarchically superior commits the crime of unauthorized access to an information system if they have the access credentials revealed to them by a subordinate in order to gain access to the system.

Sommario: 1. Svolgimento del processo; 2. Accesso disfunzionale o accesso in assoluta carenza di autorizzazioni: l'imputazione va interpretata nel modo più logico; 3. Mancata consegna delle credenziali d'accesso ed irrilevanza della gerarchia: divieto implicito ma chiaro; 4. Indifferenza rispetto al passato e al movente.

La Suprema Corte con la sentenza del 31/10/2024, n. 40295 (ud. 08/05/2024) offre un peculiare spaccato ermeneutico della fattispecie delittuosa dell'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p.. Invero, la V Sezione non si limita a ribadire i principi già più volte espressi, ma giunge ad un'interessante approfondimento su aspetti che tendono a definire con maggiore chiarezza i confini di una fattispecie sempre più attuale, in particolare in riferimento all'ambito dei rapporti di lavoro.

1. Svolgimento del processo

L'imputato accedeva al sistema informatico aziendale destinato all'archiviazione e alla gestione del parco clienti, utilizzando le credenziali di accesso di un'altra impiegata a lui subordinata. Nella formulata imputazione si contestava l'accesso abusivo ad un sistema informatico o telematico ex art. 615-ter c.p. sotto l'aspetto del c.d. "accesso disfunzionale", ossia "per scopi estranei al mandato ricevuto", e la frode informatica ex art. 640-ter c.p., oltre l'aggravante teleologica di cui all'art. 61, n. 2, c.p.

Condannato in primo grado, veniva condannato in grado d'appello per il reato di accesso abusivo ad un sistema informatico o telematico ex art. 615-ter c.p., mentre veniva assolto dal reato di frode informatica ex art. 640-ter c.p., pertanto esclusa l'aggravante della connessione teleologica di cui all'art. 61, n.2, c.p. originariamente contestata.

Interposto ricorso per la cassazione della sentenza di merito, la difesa dell'imputato affidava il gravame a diversi motivi, tutti ricondotti alla manifesta illogicità e mancanza di motivazione. E invero, le argomentazioni prospettate, miranti tutte, in estrema sintesi, a dimostrare che non si fosse trattato di un accesso abusivo, avendone il ricorrente il potere

CamminoDiritto.it
ISSN 2421-7123

nella veste di direttore e superiore della dipendente a cui aveva chiesto le credenziali anche al fine di controllarne il lavoro, che si fosse in presenza di dati sino a poco tempo prima comunque a disposizione del medesimo, che non fosse provato il divieto di accedervi o che di tale divieto fosse a conoscenza il ricorrente, che quest'ultimo avesse comunque agito per tutelare l'azienda per cui lavorava, mettendoli al sicuro.

2. Accesso disfunzionale o accesso in assoluta carenza di autorizzazioni: l'imputazione va interpretata nel modo più logico

La contestazione in imputazione del c.d. "accesso disfunzionale" (ovvero da parte di soggetto teoricamente autorizzato, ma che lo compia per finalità diverse da quelle per cui potrebbe farlo), non importa la nullità della sentenza ex art. 522 c.p.p. nel caso di riconosciuto accesso non autorizzato per carenza assoluta di permessi, quandunque mai contestato in tali termini. Invero, laddove l'imputazione abbia contestato l'ingresso in una banca dati attraverso le credenziali fornite da altri che legittimamente ne disponeva, non può assolutamente dirsi che nel capo di imputazione non fosse contenuta una tale accusa.

Ciò anche nel caso in cui nella rubrica sia anche indicato il cosiddetto "accesso disfunzionale", ciò non implicando che l'accusa poi accertata in giudizio non fosse anche contestata, trattandosi semmai solo di scarsa chiarezza del capo d'imputazione.

Invero, la scarsa chiarezza e persino la contraddittorietà dell'accusa, se non eccepita nei termini di legge[1], non esclude che il giudice di merito interpreti la contestazione nel modo più logico, dal momento che non avrebbe senso affermare che l'imputato avesse diritto ad accedere ad un sistema informatico di cui non aveva le credenziali di ingresso, tanto da avere necessità di chiederle ad altro personale.

3. Mancata consegna delle credenziali d'accesso ed irrilevanza della gerarchia: divieto implicito ma chiaro

Nel caso di un sistema informatico protetto da credenziali, è evidente che vi siano ragioni di segretezza da tutelare e, pertanto, è necessario che si lasci traccia di chi vi acceda.

Ogni soggetto abilitato detiene le sue credenziali d'accesso proprio perché si tratta di dati che il titolare reputa debbano essere protetti, limitando l'accesso a chi venga dotato delle dette credenziali e facendo sì che sia lasciata traccia digitale dei singoli accessi e di chi li esegua.

L'unica logica spiegazione desumibile dalla protezione di sistema informatico o

CamminoDiritto.it
ISSN 2421-7123

telematico con delle credenziali da parte del suo titolare è l'intenzione di non farvi accedere chicchessia, ove pure gerarchicamente sovraordinato a chi sia autorizzato a farlo.

Invero, in un contesto organizzativo di tipo lavorativo, spetta al datore di lavoro ex artt. 2086 e 2104 c.c. l'organizzazione dell'impresa da lui gestita, essendo anche i suoi collaboratori apicali comunque tenuti a rispettarne le direttive[2]. Così, rientra nella piena discrezionalità del datore di lavoro stabilire le modalità di controllo di eventuali mancanze dei dipendenti, direttamente o meno, non necessariamente mediante la propria organizzazione gerarchica[3].

Non deve ritenersi meritevole l'argomento per cui dalla sovraordinazione gerarchica discende il potere di accedere a qualsiasi luogo aziendale per controlli su chi è subordinato gerarchicamente. Dunque, non sarebbe giuridicamente corretto ritenere che un dipendente, solo perché inquadrato in una qualifica superiore, abbia automaticamente il potere di accedere a dati che, secondo la discrezionale valutazione del datore di lavoro, debbano restare nella disponibilità di alcuni dipendenti ancorché di qualifica inferiore e per giunta subordinati rispetto a chi non abbia la disponibilità delle credenziali.

Pertanto il dipendente, quandunque di livello apicale ma non destinatario delle credenziali d'accesso al sistema, viola il dovere di "osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore", di cui all'art. 2104 c.c., laddove non autorizzato acceda ad un sistema informatico o telematico di cui non aveva le credenziali.

Invero, viola le direttive (quand'anche implicite, ma chiare) del datore di lavoro il dipendente che, pur in posizione gerarchicamente sovraordinata rispetto al titolare delle credenziali di accesso ad un sistema informatico aziendale, se le faccia rivelare per farvi ingresso senza averne specifica autorizzazione, essendo sufficiente a rendere manifeste tali direttive la stessa protezione dei dati mediante credenziali di accesso[4].

Dalla indisponibilità delle credenziali d'accesso al sistema informatico o telematico, quindi, può a ragione desumersi la carenza di potere al riguardo e il divieto sebbene implicito ma chiaro imposto di chi è titolare dello ius excludendi alios.

4. Indifferenza rispetto al passato e al movente

Nessuna norma impone di comprendere le ragioni dell'accesso abusivo, risultando infondata ogni pretesa difensiva diretta ad ancorare la possibilità di acclarare il fatto di reato all'asserita necessità di ricondurlo ad un movente.

CamminoDiritto.it
ISSN 2421-7123

Le norme civili, infatti, dispongono semplicemente che il dipendente si attenga alle direttive ricevute, mentre la norma penale predica come sufficiente che avvenga l'accesso ad un sistema protetto da credenziali[5].

Di talché appare altresì del tutto irrilevante che i dati per cui l'accesso abusivo si è realizzato fossero sino a poco tempo prima in liberi accesso e consultazione, secondo le pregresse disposizioni datoriali. Invero, dal passaggio dalla libera consultazione alla limitazione dei privilegi d'accesso deve logicamente trarsi il mutato volere del titolare e il pieno esercizio dello ius excludendi alios.

Poi, la deduzione per cui i dati presenti nel sistema siano rimasti a disposizione del reo, anche su un supporto digitale aziendale ma pur sempre in uso allo stesso, non elide e semmai aggrava la violazione delle direttive datoriali.

Pertanto, occorre semplicemente provare il fatto che sia avvenuto l'accesso contro il volere di chi è legittimato ad escluderlo, quindi l'ingresso in un sistema inibito a chi vi si sia invece introdotto.

La Corte di cassazione con la sentenza in commento ha. quindi, ritenuto infondata la tesi difensiva affermando il principio che segue:

"Deve, in definitiva, affermarsi che viola le direttive (quand'anche implicite, ma chiare) del datore di lavoro il dipendente che, pur in posizione gerarchicamente sovraordinata rispetto al titolare delle credenziali di accesso ad un sistema informatico aziendale, se le faccia rivelare per farvi ingresso senza averne specifica autorizzazione: essendo sufficiente a rendere manifeste tali direttive la stessa protezione dei dati mediante credenziali di accesso".

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Nel caso di specie, neppure oggetto di rituale eccezione. L'eventuale indeterminatezza del capo d'imputazione, infatti, dà luogo ad una nullità relativa ai sensi dell'art. 181 c.p.p., sanata se non eccepita entro il termine di cui all'art. 491 c.p.p.: Cass, Sez. 5, n.4277 del 29/09/2015, dep. 2016; Sez. un., n. 15983 del 11/04/2006 (citate nella sentenza annotata).

[2] Cass, Sez. lav., n. 7295 del 23/03/2018 e n. 18165 del 16/09/2015, citate nella sentenza annotata.

[3] Cass. Sez. lav., n. 21888 del 09/10/2020 e n. 3039 del 02/03/2002, citate nella sentenza annotata.

[4] Su tale ultima parte, la sentenza annotata rimanda a Cass, Sez. 2, n. 36721 del 21/02/2008.

[5] Cass., Sez. 2, n. 36721 del 21/02/2008, citata nella sentenza annotata.

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11241