LABOR Il lavoro nel diritto

Pacini Giuridica

Commette il delitto di accesso abusivo ad un sistema informatico il superiore gerarchico che si introduce nel sistema aziendale utilizzando le password fornite da una dipendente subordinata?

di A. Galli - *17 Dicembre 2024*

Con la sentenza in commento (n. 40295 del 31 ottobre 2024), la Sezione V Penale della Corte di Cassazione si è pronunciata sulla configurabilità del delitto di accesso abusivo ad un sistema informatico di cui all'art. 615*ter* c.p. da parte del superiore gerarchico, mediante l'utilizzo delle credenziali personali di una dipendente subordinata e con il consenso di quest'ultima.

Nel caso di specie, la Suprema Corte ha ritenuto provata – anche se ai soli fini civili, per decorso del termine massimo di prescrizione – la penale responsabilità per il delitto ex art. 615*ter* c.p. di un dipendente di una struttura ricettivo-alberghiera, che aveva ottenuto da altra impiegata le credenziali per accedere al sistema informatico aziendale.

Più in particolare, i Giudici di legittimità hanno respinto le argomentazioni prospettate dalla Difesa dell'imputato, per la quale quest'ultimo, in quanto quadro con funzioni direttive e superiore della dipendente titolare delle credenziali di accesso, avrebbe avuto il potere di introdursi nel sistema informatico aziendale per controllare l'operato dei lavoratori al medesimo sottoposti (tra i quali appunto anche la titolare delle password poi utilizzate).

Gli Ermellini hanno fondato il proprio *iter* motivazionale sul combinato disposto delle norme civilistiche di cui agli artt. 2086 e 2104 c.c.

L'art. 2086, comma 1, c.c. stabilisce infatti che: "*L'imprenditore è il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori*".

L'art. 2104 c.c. dispone invece che "*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*".

Conseguentemente, secondo il Collegio giudicante, rientra nella piena discrezionalità del datore di lavoro – al quale spetta l'organizzazione e la gestione dell'impresa – stabilire le modalità di controllo dell'operato dei dipendenti e, a tal fine, lo stesso non deve necessariamente fare ricorso alla struttura gerarchica.

In altre parole, con la presente sentenza, i Giudici di legittimità hanno sostenuto come fosse errato in diritto, alla luce delle citate disposizioni civilistiche, ritenere che l'imputato avesse, per il solo fatto della propria qualifica di "superiore gerarchico", il potere di accedere a dati che, al contrario, sarebbero dovuti restare nella sola disponibilità di alcuni soggetti (per quanto subordinati all'imputato ricorrente), sulla base della valutazione discrezionale operata dal datore di lavoro.

Dunque, la carenza in capo all'imputato del potere di accedere al sistema aziendale era ricavabile, secondo la Suprema Corte, dalla – mera – indisponibilità da parte dello stesso delle relative credenziali e dalla necessità che il medesimo ha avuto di avvalersi della password di altra dipendente per consultare i dati informatici.

In conclusione, gli Ermellini hanno enunciato il principio di diritto per il quale viola le direttive 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 la specifica autorizzazione.

Tale decisione si pone, dunque, in linea con l'orientamento giurisprudenziale consolidatosi in materia, per il quale integra il delitto di accesso abusivo ad un sistema informatico la condotta di colui che acceda (o si mantenga) in un sistema protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema medesimo per delimitarne oggettivamente l'accesso a terzi (*ex multis*, Cass. Pen., Sez. II, 20 novembre 2014, n. 52680).

Secondo infatti la Giurisprudenza di legittimità maggioritaria (Cass. Pen., Sez. Un, 26 marzo 2015, n. 17325), la norma in commento tutela non soltanto il c.d. domicilio informatico, inteso quale luogo nel quale (al pari che in quello c.d. fisico) l'individuo esplica liberamente la propria personalità, bensì offre una tutela più ampia, che si concreta nello *ius excludendi* del titolare del sistema informatico, indipendentemente dalla circostanza che i dati in esso racchiusi abbiano contenuto personale.

In altri termini, per l'orientamento richiamato, con la fattispecie incriminatrice di cui trattasi il legislatore avrebbe esteso al domicilio informatico lo *ius excludendi* del titolare che caratterizza il domicilio fisico, al fine di assicurare protezione all'ambiente "telematico", quale luogo inviolabile delimitato da confini "virtuali", costituzionalmente garantito, che contiene dati personali meritevoli di riservatezza e di tutela rispetto ad altrui ingerenze ed intrusioni.

D'altra parte, proprio con riferimento al contesto aziendale, quale quello oggetto della pronuncia in analisi, la Suprema Corte ha sostenuto, ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico, che la protezione del sistema possa essere adottata anche con misure di carattere organizzativo che disciplinino le modalità di accesso, consentito esclusivamente dal titolare per determinate finalità ovvero per il raggiungimento degli scopi aziendali (Cass. pen., Sez. V, 18 dicembre 2012, n. 18497).

Arianna Galli, avvocato in Milano

Visualizza il documento: Cass. pen., sez. V^a^, 31 ottobre 2024, n. 40295