L'accesso abusivo al sistema informatico

Diritto penale Delitti

Valerio de Gioia

23 | 01 | 2025

Con sentenza n. 2905 del 23 ottobre 2024-23 gennaio 2025, la quinta sezione penale della Corte di Cassazione ha affermato che, ai fini della configurabilità del reato previsto dall'art. 615-ter c.p., la protezione del sistema può essere adottata anche con misure di carattere organizzativo. Difatti: - in considerazione della lettera della norma, che punisce sia chi si introduce abusivamente in un sistema informatico o telematico, sia chi vi si mantiene contro la volontà, espressa o tacita, di chi ha li diritto di escluderlo; - e considerando, pure alla luce della sua collocazione nella sezione concernente i delitti contro la inviolabilità del domicilio, che essa tutela «molti beni giuridici ed interessi eterogenei, quali il diritto alla riservatezza, diritti di carattere patrimoniale, come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo, interessi pubblici rilevanti, come quelli di carattere militare, sanitario nonché quelli inerenti all'ordine pubblico ed alla sicurezza, che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate», tra cui - senza «alcun dubbio» - «particolare rilievo assume la tutela del diritto alla riservatezza e, quindi, la protezione del domicilio informatico», tanto che il precetto «prevede uno ius excludendí alíos»; - si è osservato che «la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sé, perché non si tratta di un illecito caratterizzato dalla effrazione dei sistemi protettivi, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone»; e che «l'illecito è caratterizzato dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio e come è testimoniato dalla seconda parte dell'art. 615-ter c.p., comma 1», il cui disposto è stato poco sopra riportato (Cass. pen., sez. V, 8 luglio 2008, n. 37322, che richiama, tra le altre Cass. pen., sez. V, 7 novembre 2000, n. 12732). Da tale premessa si è coerentemente tratto che, pur essendo «*necessario che l'accesso al sistema informatico non sia aperto a tutti, come talora avviene soprattutto quando si tratti di sistemi telematici*», «*ai fini della configurabilità del delitto, assum[e] rilevanza qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi*» (Cass. pen., sez. V, n. 12732/2000, cit., che ha ritenuto «certamente corretta, in questa prospettiva, la distinzione operata [...] tra le banche dati offerte al pubblico a determinate condizioni e le banche dati destinate a un'utilizzazione privata esclusiva, come i dati contabili di un'azienda», soggiungendo che «in questo secondo caso è evidente, infatti, che, anche in mancanza di meccanismi di protezione informatica, commette il reato la persona estranea all'organizzazione che acceda ai dati senza titolo o autorizzazione, essendo implicita, ma intuibile, la volontà dell'avente diritto di escludere gli estranei. D'altro canto, l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva»; cfr. pure Cass. pen., sez. V, n. 37322/2008, cit., la quale ha ribadito che «la protezione del sistema può essere adottata anche con misure di carattere organizzativo», quali quelle che disciplinano «le modalità di accesso ai locali ove il sistema è ubicato ed indic[a]no le persone abilitate all'utilizzo dello stesso», puntualizzando che «naturalmente l'accesso al sistema è consentito dal titolare per determinate finalità, ovvero il raggiungimento degli scopi aziendali, cosicché se il titolo di legittimazione all'accesso viene dall'agente utilizzato per finalità diverse da quelle consentite non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione»). Tale prospettiva ermeneutica è conforme ai princìpi posti dalle Sezioni Unite a proposito dell'incriminazione in discorso. In particolare, Cass. pen., sez. un., n. 4694/2011, nell'affermare, per l'appunto, che «integra il delitto previsto dall'art. 615-ter c.p.» la condotta di «colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema», hanno ritenuto che il delitto ricorre «sia allorquando [l'agente] violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema [...] sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito». Anche l'Alto Consesso - dopo aver richiamato, nei medesimi termini poco sopra esposti, le condotte punite dall'art. 615-ter c.p. -

© Copyright 2026. All Rights Reserved • La Tribuna srl • Largo Erfurt 7 - 29122 Piacenza • Registrazione ROC 24492 •

ha attribuito rilievo, al fine di individuare il quid del reato, al «profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro) sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito. In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta» (ivi). Ancora, le Sezioni Unite hanno rimarcato che: «il dissenso tacito del dominus loci non viene desunto dalla finalità (quale che sia) che anima la condotta dell'agente, bensì dall'oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema»; «il giudizio circa l'esistenza del dissenso del dominus lo deve assumere come parametro al sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal dominus stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della condotta, soggettivamente intesa. Vengono in rilievo, al riguardo, quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, da prendere necessariamente in considerazione, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati» (ivi). Il piano argomentativo qui riportato ha trovato conferma anche nella giurisprudenza successiva alla pronuncia delle Sezioni Unite appena menzionata, la quale ha ribadito che, «ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico o telematico, la protezione del sistema può 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; cfr. pure Cass. pen., sez. II, 20 novembre 2014, n. 52680: «Integra il delitto di cui all'art. 615-ter c.p. la condotta di colui che acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare dell'elaboratore per delimitarne oggettivamente l'accesso»). Né esso può dirsi confutato da Cass. pen., sez. un., 18 maggio 2017, n. 41210, che hanno puntualizzato il dictum di Cass. pen., sez. un., n. 4694/2011, cit., affermando che integra il delitto in discorso «la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita» (Cass. pen., sez. un., 18 maggio 2017, n. 41210).

© Copyright 2026. All Rights Reserved • La Tribuna srl • Largo Erfurt 7 - 29122 Piacenza • Registrazione ROC 24492 • Pagina 2/2