diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p.

Autore: Alù Angelo
In: Giurisprudenza commentata

La fattispecie criminosa prevista dall'art. 615-ter c.p. ha alimentato un vivace dibattito interpretativo culminato nella recente pronuncia del 2015 delle Sezioni Unite che approfondisce la questione relativa alla concreta individuazione del luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p., al fine di elaborare un criterio ermeneutico utilizzabile per superare le incertezze interpretative esistenti, alla luce di orientamenti divergenti nella ricostruzione della portata applicativa della norma.

In particolare:

1. una prima tesi riteneva che il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico doveva essere individuato nel luogo in cui era materialmente collocato il server che elaborava e controllava le credenziali di autenticazione del cliente.

2. un diverso orientamento, invece, ai fini del perfezionamento del reato, focalizzava il luogo in cui venivano inseriti i dati idonei ad entrare nel sistema, ossia dove si trovava l'utente che operava illecitamente sulla postazione remota, anche se si trattava di luogo diverso da quello in cui materialmente era collocato il server.

Naturalmente, le prospettate impostazioni interpretative configuravano differenti soluzioni applicative in ordine alla concreta determinazione della competenza per territorio, atteso che nel primo caso si affermava la competenza del tribunale del luogo in cui si trovava fisicamente il server, mentre nel secondo caso si sosteneva la competenza per territorio del tribunale del luogo nel quale il soggetto agente si connetteva al sistema effettuando l'accesso abusivo.

Diritto & Diritti ISSN 1127-8579

L'intervento delle S.U. è diretto a risolvere il contrasto ermeneutico nella concreta ricostruzione dell'ambito applicativo dell'art. 615-ter c.p. al fine di superare le problematiche esistenti.

Un'efficace ed esaustiva comprensione delle argomentazioni contenute nella sentenza del 26 marzo 2015, n. 17325 rende necessaria una preliminare analisi della fattispecie criminosa disciplinata dalla norma menzionata.

In primo luogo, l'art. 615-ter c.p. (collocato all'interno della Sezione IV, Capo III, Titolo XII, Libro II del Codice Penale) è stato introdotto per assicurare un'efficace protezione dei dati personali conservati in un sistema informatico al riparo da intrusioni altrui, al fine di adeguare l'ordinamento italiano alle prescrizioni previste dalla Raccomandazione
No. R. (89) del Consiglio di Europa del 1989 (adottata dal Comitato dei Ministri il 18/1/1989).

In tale prospettiva, il bene giuridico tutelato dall'art. 615-ter può essere individuato nella protezione del "domicilio informatico", quale bene costituzionalmente protetto, in quanto diretta esplicazione della sfera individuale, dal combinato disposto degli artt. 2 e 14 Cost., la cui portata applicativa è ulteriormente rafforzata, a livello transnazionale, dall'art. 7 della Carta dei Diritti fondamentali dell'Unione europea e dall'art. 8 CEDU.

Tale norma, pertanto, è diretta a **garantire l'inviolabilità del domicilio, inteso come luogo, anche virtuale, dove l'individuo esplica liberamente la sua personalità in tutte le sue dimensioni e manifestazioni**.

Al riguardo, giova precisare che, secondo la consolidata giurisprudenza di legittimità, l'art. 615-ter c.p. offre una tutela ampia, comprensiva e anticipata che si sostanzia nel cd. "ius excludendi alios", avente ad oggetto tutti i dati raccolti nei sistemi informatici protetti, indipendentemente dal loro contenuto, purché attinenti alla sfera di pensiero o alle attività, lavorative e non, dell'utente, in modo da assicurare una

Diritto & Diritti ISSN 1127-8579

protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-patrimoniali (a titolo esemplificativo, si veda Cass., Sez. VI, sentenza del 1999, n. 3067).

Ciò premesso, il delitto di cui all'art. 615-ter c.p. integra **un reato di mera condotta che si perfeziona con la violazione del domicilio informatico, mediante l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi un'effettiva lesione della riservatezza degli utenti** (Cass., V, sentenza del 2007, n. 11689).

Più precisamente l'art. 615-ter c.p. **punisce a titolo di dolo generico le condotte non solo di chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ma anche di chi vi si trattiene contro la volontà, espressa o tacita, del titolare che ha il diritto di escluderlo**.

Tale principio di diritto è stato autorevolmente affermato dalle S.U. della Cassazione, con sentenza del 2012, n. 4694/2012, secondo cui 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 e 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".

Ciò che conta ai fini della configurabilità del delitto punito dall'art. 615-ter c.p., infatti, è il solo dato oggettivo dell'accesso e del trattenimento nel sistema informativo, violando le prescrizioni del titolare, mediante condotte dirette a realizzare operazioni di natura ontologicamente diversa da quelle per le quali sia consentito l'accesso e risultando irrilevanti le finalità concretamente perseguite mediante l'accesso (Cass., Sez. V, sentenza del 2015, n. 10083).

Inoltre, il delitto di accesso abusivo di cui all'art. 615-ter c.p. può concorrere con il reato di frode

Diritto & Diritti ISSN 1127-8579

informatica di cui all'art. 640-ter c.p., in quanto sono diversi sia i beni giuridici tutelati sia le condotte sanzionate dalle due norme.

Mentre l'art. 615-ter c.p. tutela il domicilio informatico anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, l'art. 640-ter c.p. richiede, come elemento costitutivo necessario della fattispecie, la manipolazione del sistema, la cui configurabilità deve escludersi nel reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica (Cass., V, sentenza del 2009, n. 1727).

Sempre la Suprema Corte ha affermato che il reato punito dall'art. 615-ter c.p. può essere aggravato dalla circostanza di cui all'art. 7 D.L. 13 maggio 1991, n. 152, convertito nella Legge 12 luglio 1991, n. 203 (consistente nell'aver commesso il fatto avvalendosi delle condizioni previste dall'art. 416-bis c.p., ovvero al fine di agevolare l'attività delle associazioni mafiose), qualora il soggetto agente commetta la condotta criminosa al fine "di apprendere notizie sulle sorti di un procedimento penale in relazione al reato di associazione mafiosa addebitato all'imputato, in quanto la captazione di dette informazioni non può essere preordinata alla salvaguardia di un interesse esclusivamente personale, ma costituisce obiettivamente un vantaggio non solo per il soggetto che riceve l'informazione ma per tutta l'associazione, posto che la lesione della segretezza crea un vulnus nelle indagini, di cui possono avvantaggiarsi gli associati, contrastando con comportamenti o atti illegittimi i fatti destinati a restare segreti" (Cass., Sez. V, sentenza del 2004, n. 23134).

Per quanto riguarda il luogo di consumazione del delitto punito dall'art. 615-ter c.p., si è registrato un contrasto interpretato culminato nell'intervento delle S.U. con sentenza del 26 marzo 2015, n. 17325, che ha determinato il superamento del precedente indirizzo giurisprudenziale, in base al quale il luogo di consumazione del reato doveva essere individuato in quello in cui era materialmente collocato il server preposto ad elaborare e controllare le credenziali di autenticazione del cliente (Cass., Sez. I, sentenza del 2013, n. 40303).

In particolare, secondo tale impostazione non avallata dalle Sezioni Unite del 2015, valorizzando, ai fini

Diritto & Diritti ISSN 1127-8579

della integrazione del reato, la concreta condotta abusiva di accesso al sistema informatico o telematico altrui e individuando il momento perfezionativo del delitto nel momento in cui il soggetto agente entrava nel sistema, o vi permaneva, così violando il domicilio informatico, il luogo di consumazione veniva determinato nel luogo in cui si trovava materialmente il server violato che controllava le credenziali di autenticazione oltrepassate dal soggetto agente senza un valido titolo abilitativo.

I giudici ermellini, con la citata sentenza del 2015, n. 17325, prendendo le distanze dal menzionato orientamento interpretativo, chiariscono in primo luogo il significato di "sistema informatico", valorizzando la nozione delineata dall'art. 1 della Convenzione Europea di Budapest del 23 novembre 2001 che definisce il sistema informatico come "qualsiasi apparecchiature o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati", per indicare
con tale termine il complesso di "di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche parziale) di tecnologie informatiche che sono caratterizzate, per mezzo di una attività di "codificazione" e "decodificazione", dalla "registrazione" o "memorizzazione" tramite impulsi elettronici, su supporti adeguati, di "dati", cioè, di rappresentazioni elementari di un fatto, effettuata attraversi simboli (bit) in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme più o meno vasto di informazioni organizzate secondo una logica che consente loro di esprimere un particolare significato per l'utente" (Cass., Sez. VI, sentenza del 1999, n. 3067).

Ciò posto, le S.U. ritengono che risulterebbe del tutto arbitrario effettuare un'irragionevole scomposizione tra i server periferici e il server centrale, atteso che il sistema telematico deve considerarsi in senso unitario, comprensivo del server di gestione, contenente la banca dati ed i terminali ad esso collegati o interconnessi tra loro, "essendo coordinato da un software di gestione che presiede al funzionamento della rete, alla condivisione della banca dati, alla archiviazione delle informazioni, nonché alla distribuzione e all'invio dei dati ai singoli terminali interconnessi".

Tutto ciò comporta che "la nozione di accesso in un sistema informatico non coincide con l'ingresso all'interno del server fisicamente collocato in un determinato luogo, ma con l'introduzione telematica o

Diritto & Diritti ISSN 1127-8579

virtuale, che avviene instaurando un colloquio elettronico o circuitale con il sistema centrale e con tutti i terminali ad esso collegati.”

Pertanto, secondo i giudici di legittimità, **la consumazione del reato di cui all’art. 615 ter c.p. avviene nel momento e nel luogo dove si verifica l’accesso al sistema dal terminale cosiddetto periferico**, in quanto è proprio in tal frangente che il soggetto agente pone in essere l’unica azione materiale e volontaria consistente nella digitazione da remoto delle credenziali di autenticazione che gli consente di eseguire la procedura di login in modo da accedere al sistema, superando le misure di sicurezza predisposte dal titolare, risultando del tutto irrilevante il luogo in cui si trova il server.

https://www.diritto.it/il-reato-di-accesso-abusivo-ad-un-sistema-informatico-o-telematico-di-cui-all-art-615-ter-c-p/

Diritto & Diritti ISSN 1127-8579