

“ACCESSO ABUSIVO A SISTEMA INFORMATICO DELL'AUTORIZZATO” - Cass. S.U. 4694/2012

Corte di cassazione - Sezione Unite - Sentenza 7 febbraio 2012 n.4694

PRINCIPIO. *Commette il reato di accesso abusivo a un sistema informatico chi possiede la password del database ma la utilizza per scopi diversi, e quindi illeciti, da quelli consentiti e previsti dal titolare del sistema.*

FATTO. Un carabiniere munito di regolare password per accedere al database investigativo riservato agli appartenenti dell'Arma (S.D.I. “Sistema di Indagine”) si è servito di queste credenziali di autenticazione, non al fine della conduzione di un'indagine ufficiale, bensì per meri scopi privati, in particolare per svelare informazioni riservate ad una sua conoscente per aiutarla in vista di un procedimento di separazione.

DIRITTO. Le Sezioni Unite della Cassazione, aderendo ad un orientamento restrittivo della quinta sezione penale, hanno precisato che “*integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema*” **Cass. S.U. 7 febbraio 2012 n. 4694**

La Quinta sezione del Supremo consesso nel 2008 (Cassazione penale, sez. V, sentenza 01.10.2008 n° 37322) aveva ben precisato le ragioni di diritto di tale orientamento.

“Il fatto storico nella sua materialità, ben ricostruito dai giudici di merito, non è in realtà contestato. I due professionisti, che erano ancora soci dello Studio associato S. non ancora sciolto, effettivamente si introdussero nel sistema informatico dello studio costituito da due servers e da due computers portatili, sui quali trasferirono i dati contenuti nei servers; i due portatili furono poi portati in altro luogo ove i dati vennero copiati ed, infine, i computers furono restituiti allo studio a richiesta del liquidatore.

Orbene il fatto contestato costituisce violazione dell'articolo 615 ter c.p. perché si tratta di un accesso abusivo ad un sistema informatico.

È necessario ricordare che la norma in esame tutela, secondo la più accreditata dottrina, 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 i beni e gli interessi tutelati non vi è alcun dubbio, come già osservato dalla Suprema Corte

(Cass., Sez. VI penale, 4 ottobre 1999-14 dicembre 1999, n. 3067, CED 3067), che particolare rilievo assume la tutela del diritto alla riservatezza e, quindi, la protezione del domicilio informatico, visto quale estensione del domicilio materiale.

Tanto si desume dalla lettera della norma che non si limita soltanto a tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici, ma prevede uno ius excludendi alios quale che sia il contenuto dei dati, purché attinenti alla sfera di pensiero o alla attività lavorativa dell'utente; è, quindi, evidente che da tale norma vengono tutelati anche gli aspetti economici e patrimoniali, come si è dinanzi anticipato.

D'altro canto il reato di accesso abusivo ai sistemi informatici è stato collocato dalla legge 23 dicembre 1993 n. 547, che ha introdotto nel codice penale i cosiddetti computer's crimes, nella sezione concernente i delitti contro la inviolabilità del domicilio e nella relazione al disegno di legge i sistemi informatici sono stati definiti un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli articoli 614 e 615 c.p..

Tanto premesso, la discussione che si è sviluppata nei gradi di merito in ordine alla sussistenza o meno di una protezione del sistema informatico violato appare fuori luogo, dal momento che agli imputati non è stato contestato soltanto la introduzione, ma il permanere nel sistema informatico al fine di copiare i dati ivi contenuti.

L'articolo 615 ter c.p.. infatti punisce non solo chi si introduca abusivamente in un sistema informatico, ma anche chi nello stesso si trattenga contro la volontà dell'avente diritto.

Ciò a prescindere dal fatto che nel caso di specie i sistemi di protezione dei servers, che erano quelli che custodivano i dati raccolti, esistevano, dal momento che essi non debbono consistere in strumenti tecnologici particolari, essendo sufficiente anche una semplice password, come era previsto nel caso di specie, che renda evidente la volontà dell'avente diritto di non fare accedere chiunque al sistema informatico.

Come è stato acutamente osservato (Cass., Sez. V penale, 16 giugno 2000 - 10 agosto 2000, n. 9002, CED 217734 e Cass., Sez. V penale 7 novembre 2000, Zara e da ultimo Cass., Sez. II penale, 4 maggio 2006 - 14 settembre 2006), 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.

In effetti 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 del primo comma dell'articolo 615 ter c.p., già dinanzi richiamato.

Conseguenza di tale impostazione è che la protezione del sistema può essere adottata anche con misure di carattere organizzativo che disciplinino le modalità di accesso ai locali ove il sistema è ubicato ed indichino le persone abilitate all'utilizzo dello stesso.

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”.

Cassazione penale , sez. V, sentenza 01.10.2008 n° 37322.