ROMA

FULL IMMERSION SINGOLI REATI

PENALE
PARTE
SPECIALE

Direttore Scientifico

Roberto Giovagnoli - Consigliere di Stato

Roma, 24 e 25 Giugno 2015
CARTE GEOGRAFICHE

ITA Srl
10121 Torino - Via Brofferio, 3 - Tel. (011) 56 11 426 / 56 24 402 / 54.04.97
Telefax (011) 53.01.40 - www.itasoi.it e-mail: ita@itasoi.it
Cod. Fisc. - Part. IVA - Iscr. Reg. Impr. di Torino C.C.I.A.A. 01593590605 - R.E.A. 976163

LE SEZIONI UNITE SULL'ACCESSO ABUSIVO A UN SISTEMA INFORMATICO O TELEMATICO

Cass., Sez. un., 27.10.2011 (dep. 7.2.2012), n. 4694, Pres. Lupo, Rel. Fiale, ric. C.
(è penalmente illecita la condotta di soggetto che, pur legittimato all'accesso a un sistema informatico o telematico, violi condizioni e limiti imposti dal titolare per disciplinarlo, a nulla rilevando scopi e finalità dell'accesso stesso)

[Gioacchino Romeo]

1. Il **contrasto giurisprudenziale** che le Sezioni unite hanno composto con la decisione in epigrafe riguardava la nozione di "abusività" nel reato previsto dall'art. 615-*ter*, comma primo, c.p. che punisce l'accesso abusivo a un sistema informatico o telematico: contrasto abbastanza risalente, segnalato oltre due anni or sono dall'Ufficio del massimario e rilevato anche in dottrina (G. Leo, *Accesso abusivo ad un sistema informatico o telematico*, in *Osservatorio contrasti giurisprudenziali*, in *Dir. pen. proc.* 2009, p. 443).
Nella specie un sottufficiale dei carabinieri che aveva titolo ad accedere a un sistema informatico in dotazione alle forze di polizia e contenente dati di indagine coperti da riservatezza, aveva acquisito notizie riguardanti la sfera privata e le vicende giudiziarie di svariate persone, pur non essendo stato officiato di accertamenti sul loro conto, e successivamente aveva rivelato le informazioni così apprese a una delle persone interessate e a un terzo.
La quinta sezione penale, assegnataria del ricorso proposto contro la condanna seguitane, lo aveva rimesso alla più alta istanza di giurisdizione, sul rilievo della persistenza del contrasto in ordine all'oggettività del delitto in argomento.
Le **Sezioni unite**, dopo avere dato atto dell'attualità del contrasto, hanno passato in rassegna i diversi indirizzi presenti nella giurisprudenza delle sezioni semplici, non senza aver opportunamente premesso che **le condotte punite dall'art. 615-*ter***, comma primo, c.p., **consistono**: *a*) **nell'introdursi abusivamente in un sistema informatico** o telematico protetto da misure di sicurezza (da intendere come accesso alla conoscenza di dati o informazioni contenuti nel sistema, effettuato sia da lontano, sia da vicino; *b*) **nel mantenersi nel sistema contro la volontà**, espressa o tacita, **di chi ha il diritto di esclusione** (da intendere come il fatto di chi persista nella già avvenuta introduzione, inizialmente autorizzata o casuale, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema).

2. Secondo un **primo orientamento** il **reato in argomento non sarebbe configurabile allorché il soggetto** che **abbia titolo per accedere al sistema** se ne avvalga per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente ravvisabili, ove tali finalità vengano poi effettivamente realizzate.
Si tratta di **un'interpretazione giustificata dalla necessità** di verificare la liceità della condotta esclusivamente con riguardo al suo risultato immediato, e non con riferimento a fatti successivi (l'uso illecito dei dati) che, quantunque già programmati, possono di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente, nonché **di evitare inaccettabili dilatazioni della fattispecie** riguardante il fatto di chi "abusivamente si introduce", e quindi non riferibile, per ovvi motivi di garanzia, se non agli "accessi non autorizzati" (interpretazione avallata anche in sede sovranazionale con l'uso della locuzione "accesso senza diritto" impiegata nell'art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica, ratificata con legge 18 marzo 2008 n. 48).
A tale orientamento aderiscono **le sentenze** della quinta sezione penale **20 dicembre 2007 n. 2534/2008**, in *Dir. inform*., 2009, p. 58, **29 maggio 2008 n. 26797**, in *Cass. pen*., 2009, p. 1502 e **25.6.2009 n. 40078**, in *Guida dir.*, 2009, 50, p. 67, nonché **la sentenza** della sesta sezione penale **8 ottobre 2008 n. 39290**, in *C.e.d. Cass.*, n. 242684.
Secondo un **opposto orientamento**, invece, perché sia configurabile il reato in argomento, **basta la semplice condotta del soggetto che, pur abilitato ad accedere al sistema informatico o telematico, vi si introduca** con la *password* di servizio per raccogliere dati protetti per fini estranei alle ragioni di istituto e agli scopi insiti nella protezione dell'archivio informatico, **utilizzando il sistema per obiettivi diversi da quelli consentiti**.
Tale orientamento **si fonda sul rilievo che la norma punisce non soltanto l'abusiva introduzione nel sistema** (da escludere in caso di possesso del titolo di legittimazione), **ma anche l'abusiva permanenza** in esso contro la volontà di chi ha l'i*us excludendi*, da presumersi contraria in caso di perseguimento di una finalità illecita incompatibile con le ragioni per le quali l'autorizzazione all'accesso sia stata concessa. In tal senso si registrano le **sentenze** delle quinta sezione penale **7.11.2000 n. 12732**, in *Cass. pen*., 2002, p. 1015, **8.7.2008 n. 37322**, in *Dir. pen. proc*., 719, **30.9.2008 n. 1727/2009**, in *C.e.d. Cass.*, n. 242939, **13.2.2009 n. 18006**, *ivi*, n. 243602, **10.12.2009 n. 2987/2010**, *ivi*, n. 245842, **16.2.2010 n. 19463**, in *Cass. pen.*, 2011, p. 2198, **18.1.2011 n. 24583**, in *Cass. pen.*, 2011, p. 4237.

3. A fronte del contrastante quadro interpretativo delineato, le **Sezioni unite** hanno ritenuto che la questione di diritto controversa non dovesse essere riguardata sotto il profilo delle **finalità perseguite da chi accede o si mantiene nel sistema**, in quanto la volontà del titolare del diritto di escludere si connette soltanto al **dato oggettivo** della permanenza dell'agente in esso: il che significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento

al risultato immediato della condotta posta in essere, non già ai fatti successivi.
Conseguentemente, **quel che rileva è solo il profilo oggettivo dell'accesso** e del trattenimento nel sistema informatico da parte di un soggetto che **non** può considerarsi **autorizzato** ad accedervi e a permanervi sia **quando violi i limiti** risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro), sia **quando ponga in essere operazioni di natura diversa da quelle di cui egli è incaricato e in relazione alle quali l'accesso gli è consentito**.
Il giudizio sull'esistenza del dissenso del *dominus loci* non può essere, quindi, formulato in base alla direzione finalistica della condotta, ma deve assumere come parametro la sussistenza di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema.
Ne consegue che, qualora l'agente compia sul sistema un'operazione pienamente assentita dall'autorizzazione ricevuta e agisca nei limiti di questa, **il reato di cui all'art. 615-*ter* c.p. non è configurabile**, indipendentemente dallo scopo eventualmente perseguito; sicché qualora l'attività autorizzata consista anche nella acquisizione di dati informatici e l'operatore la esegua nei limiti e nelle forme consentiti dal titolare del diritto di esclusione, il delitto in esame non ricorre, anche se degli stessi dati egli si dovesse poi servire per finalità illecite.
Irrilevanti, dunque, devono considerarsi gli eventuali fatti successivi: questi, se del caso, potranno essere ricondotti ad altro titolo di reato (ad esempio, alle previsioni di cui agli artt. 326, 618, 621 e 622 c.p.).