Accesso abusivo ad un sistema informatico o telematico (Art. 615 ter c.p.)

Cass. Pen., SS.UU., sent. 24.04.2015 n. 17325
Accesso abusivo ad un sistema informatico: in quale luogo di consuma il reato (quello in cui risiede il pc da cui si effettua l'accesso illegittimo oppure quello in cui risiede il server che custodisce i dati ?)

Con la sentenza citata le Sezioni Unite analizzano la natura del reato in questione.
Il caso si caratterizza per l'accesso abusivo nel sistema informatico di un Ministero da a parte di un impiegato, al fine di effettuare visure elettroniche non pertinenti con le mansioni lavorative cui l'impiegato stesso era preposto.
Orbene, è evidente che la qualifica del delitto in parola come reato di mera condotta, oppure come reato di evento, consente di determinare quale competenza vada individuata.
La prima tesi esalta la fisicità del luogo ove è collocato il *server*, la seconda tesi invece si sofferma sul funzionamento delocalizzato di più sistemi informatici e telematici.
La Cassazione propende per la tesi del reato di condotta (e non di evento), specificando che le modalità di funzionamento dei sistemi informatici e telematici, esaltano non tanto il luogo in cui è collocato il *server*, quanto invece il fatto che debba attribuirsi maggiore rilevanza, al luogo in cui si verifica materialmente l'accesso al sistema o a più sistemi interconnessi tra loro, e cioè il luogo fisico in cui le informazioni vengono materialmente trattate dall'utente.
L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la *password* di accesso o esegue la procedura di *login*, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati e, di conseguenza il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente.

Corte di Cassazione - Sezioni Unite Penali
sentenza n. 17325 ud. 26.03.2015 - deposito del 24.04.2015

Ritenuto in Fatto

1. Il Procuratore della Repubblica presso il Tribunale di Napoli ha esercitato l'azione penale nei confronti di XX e YY in ordine al reato previsto dagli artt. 81, 110, 615-ter, secondo e terzo comma, cod. pen., perché, in concorso tra loro ed agendo la XX in qualità di impiegata della Motorizzazione civile di Napoli, si introducevano abusivamente e ripetutamente nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti per effettuare visure elettroniche che esulavano dalle mansioni della imputata ed interessavano lo VV (amministratore di una agenzia di pratiche automobilistiche).
Con sentenza in data 2 dicembre 2013, il Giudice della udienza preliminare del Tribunale di Napoli ha dichiarato la propria incompetenza per territorio ritenendo competente il Giudice del Tribunale di Roma in ragione della ubicazione della banca-dati della Motorizzazione civile presso il Ministero delle Infrastrutture e dei Trasporti con sede in Roma.
Chiesto il rinvio a giudizio da parte del Procuratore della Repubblica per entrambi gli imputati, il Giudice della udienza preliminare del Tribunale di Roma, con ordinanza del 16 giugno 2014, ha sollevato conflitto negativo di competenza per territorio ritenendo che il luogo di consumazione del

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

reato di accesso abusivo ad un sistema informatico dovesse radicarsi ove agiva l'operatore remoto e, pertanto, a Napoli.
2. La Prima Sezione penale, cui il ricorso è stato assegnato tabellarmente, con ordinanza n. 52575 del 28 ottobre 2014, depositata il 18 dicembre 2014, rilevato un potenziale contrasto di giurisprudenza, ha rimesso gli atti alle Sezioni Unite.
Con decreto in data 23 dicembre 2014 il Primo Presidente ha assegnato il ricorso alle Sezioni Unite, fissandone per la trattazione l'odierna udienza camerale.

Considerato in Diritto

1. Il quesito posto alle Sezioni Unite è il seguente: "Se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter, cod. pen., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente".
1.1. La questione è di particolare rilievo dal momento che il reato informatico, nella maggior parte dei casi, si realizza a distanza in presenza di un collegamento telematico tra più sistemi informatici con l'introduzione illecita, o non autorizzata, di un soggetto, all'interno di un elaboratore elettronico, che si trova in luogo diverso da quello in cui è situata la banca-dati.
Gli approdi ermeneutici hanno messo in luce due opposte soluzioni che si differenziano nel modo di intendere la spazialità nei reati informatici: per alcune, competente per territorio è il tribunale del luogo nel quale il soggetto si è connesso alla rete effettuando il collegamento abusivo, per altre, il tribunale del luogo ove è fisicamente allocata la banca-dati che costituisce l'oggetto della intrusione.
1.2. Una sola sentenza della Corte di cassazione ha approfondito il tema in esame, individuando la competenza territoriale nel luogo ove è allocato il server (Sez. 1, n. 40303 del 27/05/2013, Martini, Rv. 257252).
Secondo tale impostazione, ciò che rileva ai fini della integrazione del delitto è il momento in cui viene posta in essere la condotta che si connota per l'abusività (inconferenti essendo le finalità perseguite) che si perfeziona quando l'agente, interagendo con il sistema informatico o telematico altrui, si introduce in esso contro la volontà di chi ha il diritto di estromettere l'estraneo. Posta la centralità del jus excludendi, la fattispecie si perfeziona nel momento in cui il soggetto agente entra nel sistema altrui, o vi permane, in violazione del domicilio informatico, sia che vi si introduca contro la volontà del titolare sia che vi si intrattenga in violazione delle regole di condotta imposte. Il delitto può, di conseguenza, ritenersi consumato solo se l'agente, colloquiando con il sistema, ne abbia oltrepassato le barriere protettive o, introdottosi utilizzando un valido titolo abilitativo, vi permanga oltre i limiti di validità dello stesso.
Deriva che l'accesso si determina nel luogo ove viene effettivamente superata la protezione informatica e si verifica la introduzione nel sistema e, quindi, dove è materialmente situato il server violato, l'elaboratore che controlla le credenziali di autenticazione del client.
Il luogo di consumazione del reato non è dunque quello in cui vengono inserite le credenziali di autenticazione, ma quello in cui si entra nel server dal momento che la procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema.
Nella ipotesi di accesso da remoto, l'attività fisica viene esercitata in luogo differente da quello in cui si trova il sistema informatico o telematico protetto, ma è certo che il client invia le chiavi logiche al server web il quale le riceve "processandole" nella fase di validazione che è eseguita unicamente all'interno dell'elaboratore presidiato da misure di sicurezza.
In sostanza, l'opzione ermeneutica che ha fissato presso il server il luogo di consumazione del reato fa leva sulla constatazione che l'effettivo ingresso di cui trattasi si verifica solo presso il sistema centrale con il superamento delle barriere logiche dopo la immissione delle credenziali di autenticazione da remoto. Altra sentenza (Sez. 3, n. 23798 del 24/05/2012, Casalini, Rv. 253633),

pur senza approfondire, ha affermato, in riferimento al diverso reato di frode informatica, che la competenza territoriale deve essere individuata nel luogo in cui si trova il server all'interno del quale sono archiviati i dati oggetto di abusivo trattamento.
1.3. Un significativo segnale di mutamento in ordine alla riflessione giurisprudenziale sul luogo di consumazione del reato di accesso abusivo a sistema informatico può cogliersi in una decisione (Sez. 1, n. 34165 del 15/06/2014, De Bo, non massimata); la Corte, nel risolvere il conflitto di competenza sollevato dall'autorità giudiziaria del luogo di digitazione della password di accesso alle risorse informatiche, ha rilevato come la questione (non conferente nel caso in esame) fosse fondata su argomenti giuridici e scientifici meritevoli di attento esame critico e, quindi, di ulteriore analisi in sede di ricostruzione dell'elemento oggettivo del reato di cui all'art. 615-ter cod. pen. La ordinanza di rimessione alle Sezioni Unite - dopo avere evidenziato che il client ed il server sono componenti di un unico sistema telematico - osserva che l'accesso penalmente rilevante inizia dalla postazione remota ed il perfezionamento del reato avviene nel luogo ove si trova l'utente (diverso da quello in cui è ubicato il server).
1.4. La impostazione della ricordata sentenza n. 40303 del 2013 della Corte di cassazione è criticata dal Giudice rimettente (e da parte della dottrina) che puntualizza come l'intera architettura di un sistema per la gestione e lo scambio di dati (server, client, terminali e rete di trasporto delle informazioni) corrisponde, in realtà, ad una sola unità di elaborazione, altrimenti definita "sistema telematico".
In questa prospettiva, il terminale mediante il quale l'operatore materialmente inserisce username e password è ricompreso, quale elemento strutturale ed essenziale, nell'intera rete di trattamento e di elaborazione dei dati, assumendo rilevanza il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico.
2. Prima di esaminare la questione controversa, è opportuno puntualizzare, nello stretto ambito richiesto per risolvere il quesito, la struttura della fattispecie dell'art. 615-ter cod. pen., iniziando dalla nozione di introduzione e trattenimento nel sistema.
La materia è già stata passata al vaglio delle Sezioni Unite (sent. n. 4694 del 27/10/2011, Casani, Rv. 25129) che ha precisato come le condotte descritte dalla norma sono punite a titolo di dolo generico e consistono:
a) nello introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza - da intendere come l'accesso alla conoscenza dei dati o informazioni contenute nello stesso - effettuato sia da lontano (condotta tipica dello hacker), sia da vicino (cioè da persona che si trova a diretto contatto con lo elaboratore);
b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione, da intendere come il persistere nella già avvenuta introduzione, inizialmente autorizzata o casuale, violando le disposizioni, i limiti e i divieti posti dal titolare del sistema.
2.1. Nel caso che ci occupa (almeno dagli atti in visione di questa Corte) risulta che la XX, pur avendo titolo e formale abilitazione per accedere alle informazioni in ragione della sua qualità di dipendente della competente amministrazione e di titolare di legittime chiavi di accesso, si è introdotta all'interno del sistema, in esecuzione di un previo accordo criminoso con il coimputato al fine di consultare l'archivio per esigenze diverse da quelle di servizio; pertanto, la condotta deve essere considerata di per sé illecita sin dal momento dell'accesso, essendo irrilevante la successiva condotta di mantenimento.
2.2. Per quanto concerne il bene giuridico, va ricordato che l'art. 615-ter cod. pen è stato introdotto nel nostro ordinamento in esito alla Raccomandazione del Consiglio di Europa del 1989 per assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati al riparo da ingerenze ed intrusioni altrui e rappresenta un

luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche.
Per questo la fattispecie è stata inserita nella Sezione IV del Capo III del Titolo XII del Libro II del codice penale, dedicata ai delitti contro la inviolabilità del domicilio, che deve essere inteso come luogo, anche virtuale, dove l'individuo esplica liberamente la sua personalità in tutte le sue dimensioni e manifestazioni. E' stato notato che, con la previsione dell'art. 615-ter cod. pen. il legislatore ha assicurato la protezione del domicilio informatico quale spazio ideale in cui sono contenuti i dati informatici di pertinenza della persona ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene costituzionalmente protetto; all'evidenza il parallelo con il domicilio reale - sulla cui falsariga è stata strutturata la norma - è imperfetto.
In realtà, la fattispecie offre una tutela anticipata ad una pluralità di beni giuridici e di interessi eterogenei e non si limita a preservare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma ne offre una protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-patrimoniali (Sez. 4, n. 3067 del 04/10/1999, Piersanti, Rv. 214946).
E' condivisa l'opinione secondo la quale il delitto previsto dall'art. 615-ter cod. pen. è di mera condotta (ad eccezione per le ipotesi aggravate del comma secondo, nn. 2 e 3) e si perfeziona con la violazione del domicilio informatico e, quindi, con la introduzione nel relativo sistema - senza la necessità che si verifichi una effettiva lesione del diritto alla riservatezza dei dati (Sez. 5, n. 11689 del 06/02/2007, Cerbone, Rv. 236221).
Dal momento che oggetto di tutela è il domicilio virtuale, e che i dati contenuti all'interno del sistema non sono in via diretta ed immediata protetti, consegue che l'eventuale uso illecito delle informazioni può integrare un diverso titolo di reato (Sez. 5, n. 40078 del 25/05/2009, Genchi, Rv. 244749).
2.3. Il legislatore, introducendo con la legge 23 dicembre 1993, n. 547, i cosiddetti computer's crimes, non ha enunciato la definizione di sistema informatico o telematico (forse per lasciare aperta la nozione in vista dell'evoluzione della tecnologia), ma ne ha presupposto il significato.
In argomento, l'art. 1 della Convenzione Europea di Budapest del 23 novembre 2001, definisce sistema informatico «qualsiasi apparecchiatura o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati».
La giurisprudenza ha fornito una definizione tendenzialmente valida per tutti i reati facenti riferimento alla espressione "sistema informatico", che deve intendersi come un complesso 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 (Sez. 6, n. 3067 del 04/10/1999, Piersanti, Rv. 214945).
In generale, un dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un software che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento.
Per evitare vuoti di tutela e per ampliare la sfera di protezione offerta ai sistemi informatici e telematici, è opportuno accogliere la nozione più ampia possibile di computer o unità di elaborazione di informazioni, come del resto la Corte ha già fatto in materia di carte di pagamento,

trattandosi di strumenti idonei a trasmettere dati elettronici nel momento in cui si connettono all'apparecchiatura POS (così Sez. F, n. 43755 del 23/08/2012, Chiriac, Rv. 253583).
Nell'ambito della protezione offerta dall'art. 615-ter cod. pen. ricadono anche i sistemi di trattamento delle informazioni che sfruttano l'architettura di rete denominata client-server, nella quale un computer o terminale (il client) si connette tramite rete ad un elaboratore centrale (il server) per la condivisione di risorse o di informazioni, che possono essere rese disponibili a distanza anche ad altri utenti.
La tutela giuridica è riservata ai sistemi muniti di misure di sicurezza perché, dovendosi proteggere il diritto di uno specifico soggetto, è necessario che questo abbia dimostrato di volere riservare l'accesso alle persone autorizzate e di inibire la condivisione del suo spazio informatico con i terzi.
3. La condotta illecita commessa in un ambiente informatico o telematico assume delle specifiche peculiarità per cui la tradizionale nozione - elaborata per una realtà fisica nella quale le conseguenze sono percepibili e verificabili con immediatezza - deve essere rivisitata e adeguata alla dimensione virtuale.
In altre parole, il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; l'input rivolto al computer da un atto umano consapevole e volontario si traduce in un trasferimento sotto forma di energie o bit della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni.
L'azione telematica viene realizzata attraverso una connessione tra sistemi informatici distanti tra loro, cosicché gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova; inoltre, l'operatore, sfruttando le reti di trasporto delle informazioni, è in grado di interagire contemporaneamente sia sul computer di partenza sia su quello di destinazione.
E' stato notato che nel cyberspace i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio).
Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione.
Del resto, la dimensione aterittoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (tabiet, smartphone, sistemi portatili) e del doud computing, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo.
Va comunque precisato che, se i dati oggetto di accesso abusivo sono archiviati su cloud computing o resi disponibili da server che sfruttano tali servizi, potrebbe risultare estremamente difficile individuare il luogo nel quale le informazioni sono collocate.
4. Le esposte osservazioni sono utili per risolvere la questione sottoposta alle Sezioni Unite.
In estrema sintesi, si può rilevare che le due teorie contrapposte sul luogo del commesso reato si ancorano l'una (quella della Prima Sezione della Corte di cassazione) sul concetto classico di fisicità del luogo ove è collocato il server e l'altra (quella del Giudice rimettente) sul funzionamento delocalizzato, all'interno della rete, di più sistemi informatici e telematici.
Ora - pur non sminuendo le difficoltà di trasferire al caso concreto il criterio attributivo della competenza territoriale dell'art. 8 cod. proc. pen. parametrato su spazi fisici e non virtuali - la Corte reputa sia preferibile la tesi del Giudice remittente, che privilegia le modalità di funzionamento dei sistemi informatici e telematici, piuttosto che il luogo ove è fisicamente collocato il server.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

4.1. Deve, innanzitutto, ricordarsi come l'abusiva introduzione in un sistema informatico o telematico - o il trattenimento contro la volontà di chi ha diritto di esclusione - sono le uniche condotte incriminate, e, per quanto rilevato, le relative nozioni non sono collegate ad una dimensione spaziale in senso tradizionale, ma a quella elettronica, trattandosi di sistemi informatici o telematici che archiviano e gestiscono informazioni ossia entità immateriali.
Tanto premesso, si rileva come la ricordata sentenza della Prima Sezione abbia ritenuto che l'oggetto della tutela concreta coincida con l'ambito informatico ove sono collocati i dati, cioè con il server posto in luogo noto.
Tale criterio di articolare la competenza in termini di fisicità, secondo gli abituali schemi concettuali del mondo materiale, non tiene conto del fatto che la nozione di collocazione spaziale o fisica è essenzialmente estranea alla circolazione dei dati in una rete di comunicazione telematica e alla loro contemporanea consultazione da più utenti spazialmente diffusi sul territorio.
Non può essere condivisa, allora, la tesi secondo la quale il reato di accesso abusivo si consuma nel luogo in cui è collocato il server che controlla le credenziali di autenticazione del client, in quanto, in ambito informatico, deve attribuirsi rilevanza, più che al luogo in cui materialmente si trova il sistema informatico, a quello da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente.
Va rilevato, infatti, come il sito ove sono archiviati i dati non sia decisivo e non esaurisca la complessità dei sistemi di trattamento e trasmissione delle informazioni, dal momento che nel cyberspazio (la rete internet) il flusso dei dati informatici si trova allo stesso tempo nella piena disponibilità di consultazione (e, in certi casi, di integrazione) di un numero indefinito di utenti abilitati, che sono posti in condizione di accedervi ovunque.
Non è allora esatto ritenere che i dati si trovino solo nel server, perché nel reato in oggetto l'intera banca dati è "ubiquitaria", "circolare" o "diffusa" sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso.
A dimostrazione della unicità del sistema telematico per il trattamento dei dati, basti considerare che la traccia delle operazioni compiute all'interno della rete e le informazioni relative agli accessi sono reperibili, in tutto o in parte, sia presso il server che presso il client.
Né può in contrario sostenersi, come afferma l'orientamento che in questa sede si ritiene di non condividere, che le singole postazioni remote costituiscano meri strumenti passivi di accesso al sistema principale e non facciano altrimenti parte di esso.
4.2. Da un punto di vista tecnico-informatico, il sistema telematico deve considerarsi unitario, 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.
Consegue che è arbitrario effettuare una irragionevole scomposizione tra i singoli componenti dell'architettura di rete, separando i terminali periferici dal server centrale, dovendo tutto il sistema essere inteso come un complesso inscindibile nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi formano parte integrante di un complesso meccanismo, che è strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del client.
I terminali, secondo la modulazione di profili di accesso e l'organizzazione della banca-dati, non si limitano soltanto ad accedere alle informazioni contenute nel data base, ma sono abilitati a immettere nuove informazioni o a modificare quelle preesistenti, con potenziale beneficio per tutti gli utenti della rete, che possono fruire di dati più aggiornati e completi per effetto dell'interazione di un maggior numero di operatori.

Alla luce di questa considerazione, va focalizzata la nozione di accesso in un sistema informatico, che non coincide con l'ingresso all'interno del server fisicamente collocato in un determinato luogo, ma con l'introduzione telematica o virtuale, che avviene instaurando un colloquio elettronico o circuitale con il sistema centrale e con tutti i terminali ad esso collegati.
L'accesso inizia con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il client e il server.
L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la password di accesso o esegue la procedura di login, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati.
Da tale impostazione, coerente con la realtà di una rete telematica, consegue che il luogo del commesso reato si identifica con quello nel quale dalla postazione remota l'agente si interfaccia con l'intero sistema, digita le credenziali di autenticazione e preme il testo di avvio, ponendo così in essere l'unica azione materiale e volontaria che lo pone in condizione di entrare nel dominio delle informazioni che vengono visionate direttamente all'interno della postazione periferica.
Anche in tal senso rileva non il luogo in cui si trova il server, ma quello decentrato da cui l'operatore, a mezzo del client, interroga il sistema centrale che gli restituisce le informazioni richieste, che entrano nella sua disponibilità mediante un processo di visualizzazione sullo schermo, stampa o archiviazione su disco o altri supporti materiali.
Le descritte attività coincidono con le operazioni di "trattamento", compiute sul client, che l'art. 4, lett. a), d.lgs. 30 giugno 2003, n. 196 (codice della privacy) definisce come «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati».
La condotta è già abusiva (secondo la clausola di antigiuridicità speciale) nel momento in cui l'operatore non autorizzato accede al computer remoto e si fa riconoscere o autenticare manifestando, in tale modo, la sua volontà di introdursi illecitamente nel sistema con possibile violazione della integrità dei dati.
Deve precisarsi in ogni caso che, se il server non risponde o non valida le credenziali, il reato si fermerà alla soglia del tentativo punibile.
Nelle ipotesi, davvero scolastiche e residuali, nelle quali non è individuabile la postazione da cui agisce il client, per la mobilità degli utenti e per la flessibilità di uso dei dispositivi portatili, la competenza sarà fissata in base alle regole suppletive (art. 9 cod. proc. pen.).
4.3. Il luogo in cui l'utente ha agito sul computer - che nella maggior parte dei casi, è quello in cui si reperiscono le prove del reato e la violazione è stata percepita dalla collettività - è consono al concetto di giudice naturale, radicato al focus commissi delicti di cui all'art. 25 Cost.
La Corte costituzionale, infatti, non ha mancato di sottolineare al riguardo (v. sentenza n. 168 del 2006) come il predicato della "naturalità" del giudice finisca per assumere nel processo penale «un carattere del tutto particolare, in ragione della "fisiologica" allocazione di quel processo nel locus commissi delicti», giacché la «celebrazione di quel processo in "quel" luogo, risponde ad esigenze di indubbio rilievo, fra le quali, non ultima, va annoverata quella - più che tradizionale - per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati». In tale cornice, se l'azione dell'uomo si è realizzata in un certo luogo - sia pure attraverso l'uso di uno strumento informatico e, dunque, per sua natura destinato a produrre flussi di dati privi di una loro "consistenza territoriale" - non v'è ragione alcuna per ritenere che quel "fatto", qualificato dalla

legge come reato, non si sia verificato proprio in quel luogo, così da consentire la individuazione di un giudice anche "naturalisticamente" (oltre che formalmente) competente. Predicato, quello di cui si è detto, che, al contrario, non potrebbe ritenersi affatto soddisfatto ove si facesse leva sulla collocazione, del tutto casuale, del server del sistema violato.
4.4. D'altra parte, che il fulcro della attenzione normativa sia stato, per così dire, allocato nel luogo in cui si trova ad operare l'autore del delitto - evocando, dunque, una sorta di sincretismo tra la localizzazione dell'impianto informatico utilizzato per realizzare il fatto-reato e la persona che, proprio attraverso quell'impianto, accede e dialoga col sistema nella sua indefinibile configurazione spaziale - lo si può desumere anche dal modo in cui risultano strutturate le circostanze aggravanti previste dal comma secondo dell'art. 615-ter cod. pen.
Se si considera, infatti, l'aggravante di cui al numero 2 del predetto comma, non avrebbe senso alcuno immaginare una competenza per territorio saldata al luogo - in ipotesi del tutto eccentrico rispetto al "fatto" - in cui si trova il server, visto che è proprio l'attività violenta dell'agente (e, dunque, la relativa collocazione territoriale) a specificare, naturalisticamente, il locus commissi delicti. Allo stesso modo, è sempre il luogo in cui si trova ed opera l'agente ad essere quello che meglio individua il "fatto", ove da esso sia derivata, a norma del numero 3, la interruzione, la distruzione o il danneggiamento del sistema o di qualche sua componente: è l'operazione di manipolazione, infatti (si pensi alla introduzione di un virus) che qualifica, specificandola in chiave aggravatrice, la condotta punibile, con l'ovvia conseguenza che è l'azione umana (e non altro) a determinare il "fatto" e con esso il suo riferimento spazio-temporale. Circostanze, quelle testé evidenziate, che valgono anche per l'aggravante dell'abuso della qualità pubblica dell'autore del fatto di cui al numero 1, posto che - ancora una volta - è sempre la condotta di accesso a indicare "chi", "dove" e "quando" hanno realizzato la fattispecie incriminata, qualificandola "abusiva" in ragione delle specifiche disposizioni che regolano l'impiego del sistema.
5. Deve ora, per completezza, rilevarsi che la conclusione è trasferibile alla diversa ipotesi nella quale un soggetto facoltizzato ad introdursi nel sistema, dopo un accesso legittimo, vi si intrattenga contro la volontà del titolare eccedendo i limiti della autorizzazione.
In questo caso, non può farsi riferimento all'azione con la quale l'agente ha utilizzato le sue credenziali e dato l'avvio al sistema, dal momento che tale condotta commissiva è lecita ed antecedente alla perpetrazione del reato.
Necessita, quindi, fare leva sull'inizio della condotta omissiva che, come è stato puntualmente osservato, coincide con un uso illecito dello elaboratore, con o senza captazione di dati. L'operatore remoto, anche in questo caso, si relaziona, con impulsi elettronici e colloquia con il sistema dalla sua postazione periferica presso la quale vengono trasferiti i dati con la conseguenza che è irrilevante il luogo in cui è collocato il server per le già dette ragioni.
6. Conclusivamente, va affermato il seguente principio di diritto:
"Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente".
7. Consegue che nella specie deve essere dichiarata la competenza dell'autorità giudiziaria del Tribunale di Napoli, atteso che la condotta abusiva è stata contestata come materialmente realizzata dalla imputata XX negli uffici della Motorizzazione civile di Napoli, dove, servendosi del computer in dotazione dell'ufficio, essa si sarebbe introdotta abusivamente e ripetutamente nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti.

P.Q.M.

dichiara la competenza del G.u.p. del Tribunale di Napoli, cui dispone trasmettersi gli atti.
Così deciso il 26/03/2015
Il Componente estensore Claudia Squassoni

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

Il Presidente Giorgio Santacroce
SEZIONI UNITE PENALI
Depositato in Cancelleria 24 APR. 2015

*

Cass. Pen., sez. V, sent. 19 novembre 2014, n. 47938.
Gli scopi perseguiti dal soggetto che accede abusivamente (ex art. 615 ter c.p.) ad un sistema informatico o telematico non rilevano, essendo invece determinante il profilo oggettivo dell'accesso o della condotta del mantenersi nel sistema informatico o telematico sia che la condotta saia perpetrata da un soggetto non autorizzato, sia che acceda al sistema un soggetto in violazione delle prescrizioni impartite dal titolare del sistema stesso.

Suprema Corte di Cassazione - sezione V
Sentenza 19 novembre 2014, n. 47938

Ritenuto in fatto

Con la sentenza impugnata, in parziale riforma della sentenza del Giudice dell'udienza preliminare presso il Tribunale di Milano del 20/04/2012, veniva confermata l'affermazione di responsabilità di XX per il reato continuato di cui all'art. 615-ter cod. pen., commesso quale dipendente dell'ufficio dell'Agenzia delle Entrate di YY introducendosi con le proprie credenziali nel sistema informatico protetto dell'agenzia ed eseguendovi nel 2007 e fino al giugno del 2008, operazioni contabilmente legittime ma amministrativamente irregolari, consistite in 53 provvedimenti di sgravio e 29 comunicazioni di irregolarità. La sentenza di primo grado veniva riformata con l'assoluzione dell'imputato per insussistenza del fatto dall'imputazione del reato di cui all'art. 323 cod. pen., contestato nell'aver procurato, con le operazioni di cui sopra, ingiusto vantaggio patrimoniale allo studio professionale … e ad altri con il quali l'imputato avrebbe collaborato, e con la rideterminazione della pena in anni due di reclusione.
L'imputato ricorre sull'affermazione di responsabilità e, rammentati i principi enunciati dalle Sezioni Unite di questa Corte, nel senso della limitazione del carattere abusivo dell'accesso ad un sistema informatico ai casi nei quali vi sia un'oggettiva violazione dei limiti o delle condizioni della relativa abilitazione secondo le disposizioni impartite dal titolare del sistema, con il compimento di operazioni ontologicamente diverse da quelle per le quali l'abilitazione sia stata concessa, irrilevante essendo la finalità per la quale il soggetto attivo abbia agito, deduce violazione di legge ed illogicità della motivazione nella ritenuta natura abusiva della condotta dell'imputato per il solo fatto che lo stesso abbia effettuato gli accessi contestati in orario pomeridiano e diverso da quello di apertura dell'ufficio al pubblico, nel momento in cui le operazioni compiute rientravano nelle mansioni di ordinaria competenza del X., erano contabilmente corrette e si risolvevano in una maggiore celerità dell'azione amministrativa. Lamenta altresì travisamento del contenuto della comunicazione di notizia di reato del 13/01/2011, del verbale di audizione dell'imputato da parte dell'ufficio Audit dell'Agenzia delle Entrate e degli atti dispositivi disciplinanti l'attività lavorativa del X. sull'illiceità del lavoro pomeridiano da parte di quest'ultimo, e mancanza di motivazione sull'essere stata detta modalità concordata con i superiori dell'imputato. Deduce contraddittorietà con l'assoluzione dell'imputato dall'addebito di abuso d'ufficio, rispetto al quale l'originaria imputazione di accesso abusivo contestava specificamente l'aggravante teleologia. Lamenta infine violazione di legge rispetto alla mancanza di offensività della condotta nei confronti dell'oggetto giuridico del reato, costituito dal domicilio informatico e dalla riservatezza dei dati in esso

contenuti, considerato che l'imputato era legittimato ad accedere al sistema e non procurava alcun danno all'amministrazione finanziaria.

Considerato in diritto

Il ricorso è fondato.

Secondo i principi affermati da questa Corte e correttamente richiamati dal ricorrente in tema di configurabilità del reato di cui all'art. 615-ter cod. pen. nel caso in cui lo stesso sia contestato ad un soggetto munito di credenziali di accesso al sistema informatico, le finalità specificamente perseguite da tale soggetto sono a tali fini irrilevanti, essendo viceversa determinante il profilo oggettivo dell'accesso o del trattenimento nel sistema informatico di un soggetto che a ciò non possa ritenersi sostanzialmente autorizzato o per la violazione delle prescrizioni impartite dal titolare del sistema, quali disposizioni organizzative interne, prassi aziendali o clausole di contratti individuali di lavoro, che regolano l'accesso al sistema e stabiliscono per quali attività e per quanto tempo la permanenza nello stesso può essere protratta; ovvero per il compimento di operazioni ontologicamente diverse da quelle per le quali l'accesso è consentito (Sez. U, n. 4694 del 27/10/2011, Casani, Rv. 251269; Sez. 5, n. 15054 del 22/02/2012, Crescenzi, Rv. 252479). Nella sentenza impugnata, dandosi atto che le operazioni effettuate dall'imputato a seguito degli accessi contestati erano contabilmente legittime, e che non vi era prova di alcun vantaggio procurato con le stesse a studi professionali, le condizioni per la ravvisabilità del reato erano individuate unicamente nell'esecuzione degli accessi in orario pomeridiano e diverso da quello di apertura dell'ufficio al pubblico, ritenuta contraria alla prassi aziendale sull'uso del sistema e sulla protrazione temporale di detto uso.

Orbene, anche non voler considerare che tale contrasto del lavoro pomeridiano con le disposizioni interne veniva desunto unicamente dalla contestazione della circostanza nel verbale di audizione dell'imputato presso l'Agenzia delle entrate, e che detto verbale, prodotto dal ricorrente in quanto oggetto del motivo di travisamento della prova, risulta equivoco nella riconducibilità della contestazione ad una ritenuta illiceità intrinseca dello svolgimento del lavoro in orario pomeridiano piuttosto che alla significatività della circostanza rispetto all'originario addebito di aver favorito gli studi professionali che avevano curato le pratiche a cui afferivano le operazioni effettuate con gli accessi in esame, è assorbente la considerazione per la quale eventuali disposizioni sulla collocazione oraria degli accessi al sistema informatico, nell'ambito della giornata lavorativa del dipendente, non appaiono rilevanti quali oggetto di una violazione idonea a dar luogo alla realizzazione della fattispecie contestata. Posto invero che la relativa norma incriminatrice tutela il domicilio informatico con riguardo alle modalità che ne regolano l'accesso ai fini dell'esercizio dello jus excludendi alios da parte del titolare (Sez. 5, n. 1727 del 30/09/2008, Romano, Rv. 242938), a tale oggettività giuridica non può che farsi riferimento per l'individuazione delle disposizioni la cui infrazione integra il reato in esame. Orbene, siffatta rilevanza non può essere attribuita alle indicazioni sull'orario nel quale gli accessi possono essere effettuati, indifferenti rispetto all'esercizio della facoltà di esclusione da parte del titolare del sistema informatico nei confronti di un soggetto autorizzato all'accesso e, invece, chiaramente inerenti al solo profilo dell'organizzazione lavorativa interna dell'ufficio presso il quale il sistema è operativo. Mentre ben altra è la significatività in questa prospettiva delle diverse disposizioni riguardanti il tempo di permanenza nel sistema, in effetti espressamente individuate quali rilevanti, a differenza di quelle precedentemente citate, nella formulazione dei principi giurisprudenziali esposti in premessa. Il reato per il quale è stata affermata la responsabilità del X. con la sentenza in conclusione, in quanto ritenuto commesso esclusivamente mediante una condotta di violazione delle prime disposizioni sopra indicate, è di conseguenza insussistente. La sentenza impugnata deve pertanto essere annullata senza rinvio.

P.Q.M.

Annulla la sentenza impugnata senza rinvio perché il fatto non sussiste.

*

Cassazione Penale, Sez. V, sent. 22.05.2013 n. 22024
I dipendenti dello Stato devono sempre comportarsi *secundum legem*.
In questa pronuncia la Corte interviene in merito al fatto che il dipendente di un ufficio pubblico (Ag. Entrate) non è autorizzato a verificare la posizione di un altro contribuente avente altro domicilio fiscale, violando le prescrizioni del *dominus loci*, vale a dire della competente P.A., per violazione dell'art. 1 della L. 7 agosto 1990, n. 241. Di conseguenza l'esercizio del potere pubblico supera il vaglio della discrezionalità (possibile) e sfocia in quello della arbitrarietà (non possibile). Sussiste pertanto in tali condizioni, anche la condotta prevista e punita dall'art. 615 ter c.p.

*

Corte di Cassazione, Sez. I, sent. 27 maggio 2013 n. 40303
Accesso abusivo ad un sistema informatico o telematico.
La competenza è del giudice del luogo ove è collocato il server violato (si verifichino le successive Sezioni unite del 2015 che contraddicono questo orientamento)

*

Corte di Cassazione, Sezioni Unite, sent. 27 ottobre 2011 - dep. 7 febbraio 2012 - n. 4694
Integra la fattispecie di cui all'art. 615-ter c.p., la condotta posta in essere da soggetto che, pur 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 stesso.

*

Cass. Pen., sent. n. 24583 del 2011
Responsabilità del gruppo (holding) ai sensi della legge 231 del 2001 e ss modifiche, per il reato di accesso abusivo a sistema informatico ex art. 615 ter c.p. ?
La Cassazione ha statuito che: "la holding o altre società del gruppo possono rispondere ai sensi della legge 231/2001 anche del reato di cui all'art. 615 ter c.p. (acceso abusivo a sistema informatico), ma è necessario che il soggetto che agisce per conto delle stesse concorra con il soggetto che commette reato; non è sufficiente un generico riferimento al gruppo, per affermare la responsabilità della società ai sensi della legge 231/2001.

*

Corte di Cassazione, Sez. V, sent. 13 dicembre 2010 - dep. 21 gennaio 2011 - n. 1934
Il fatto che il sistema informatico sottoposto oggetto dell'accesso abusivo, ex art. 615 ter c.p., appartenga ad un gestore telefonico (concessionario di un pubblico servizio) non è sufficiente per la qualifica del fatto come aggravato (aggravante dell'interesse pubblico).

*

Corte d'Appello di Bologna, sent. n. 369 del 2009

E' nel prelievo indesiderato dei dati personali dal domicilio informatico che va individuato il vero bene personalissimo protetto dalla norma, e non tanto nella conoscenza o conoscibilità di quelli da parte del soggetto agente.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

*

Corte di Cassazione, Sez. V, sent. 25 giugno 2009 - dep. 14 ottobre 2009 - n. 40078

Accesso abusivo ad un sistema informatico o telematico: la "abusività" va intesa in senso oggettivo, con riferimento al momento dell'accesso ed alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza, apprestate dal titolare dello ius excludendi, al fine di impedire accessi indiscriminati.

Non hanno rilevanza la finalità che si propone l'autore e l'uso successivo dei dati che, se illeciti, integrano eventualmente un diverso titolo di reato.

*

Cass. Pen., Sez. V, sent. n. 37322 del 2008

Commette il reato di accesso abusivo ad un sistema informatico o telematico l'associato di un'associazione professionale che si introduce nel sistema informatico dell'associazione stessa ed effettui copia dell'elenco dei clienti allo scopo di sviare la clientela verso un terzo soggetto in via di costituzione.

Non ha rilevanza il fatto che l'imputato avesse diritto di accesso al sistema, perché in ogni caso l'accesso non prevedeva la sottrazione di dati importanti per lo studio associato.

Commette reato anche chi, dopo essere entrato legittimamente in un sistema, continui ad operare o a servirsi di esso oltre i limiti prefissati dal titolare e, quindi, in siffatta ipotesi ciò che si punisce è l'uso dell'elaboratore avvenuto con modalità non consentite.

Corte di Cassazione Penale

Sent. n. 37322/2008

Tizio, Caio ed Sempronio, unitamente a Mevio, avevano costituito una associazione professionale denominata Studio associato Tizio dottor ragionier, della quale il Tizio era il socio di maggioranza relativa e l'amministratore; Sempronio, Caio e Mevio, presumibilmente a causa di contrasti con il Tizio, decisero di dare vita ad una nuova associazione professionale denominata Studio Caio - Sempronio ed associati.

Nei giorni del passaggio dalla vecchia alla nuova associazione accaddero alcuni fatti che hanno originato il presente procedimento penale.

Caio e Sempronio si recarono presso la sede dello Studio Tizio, associazione della quale facevano ancora parte non essendo stata sciolta, e si introdussero nel sistema informatico dello studio prelevandone l'archivio.

Negli stessi giorni il Tizio, parlando con alcuni clienti, disse che i tre soci stavano sviando la clientela; inoltre il Tizio fece bloccare i suoi colleghi da una guardia giurata impedendo loro di entrare nello studio.

Per tali fatti il Tizio era tratto a giudizio per rispondere dei reati di cui agli articoli 595 e 393 c.p. in danno di Caio, Sempronio e Mevio, che si costituivano parti civili; Caio e Sempronio erano chiamati a rispondere della violazione degli articoli 61 n. 11, 615 ter, 646 c.p. e 35 della legge 675 del 1996 in danno di Tizio, che si costituiva parte civile.

Con sentenza del 4 maggio 2004 il Tribunale di Bergamo dichiarava Caio e Sempronio colpevoli dei reati loro ascritti e li condannava alla pena ritenuta di giustizia oltre al risarcimento dei danni ed al pagamento di una provvisionale, mentre assolveva il Tizio dal delitto di diffamazione perché il fatto non sussiste e da quello di cui all'articolo 610 c.p., così modificata la originaria imputazione, perché il fatto non costituisce reato.

Investita dagli appelli dei due imputati, anche nella loro qualità di parti civili insieme al Mevio, la Corte di Appello di Brescia, con sentenza emessa in data 27 febbraio 2007, dichiarava

inammissibile l'appello ex articolo 577 c.p.p. delle parti civili, non accoglieva l'appello agli effetti civili ed, in accoglimento dell'appello degli imputati, assolveva Caio e Sempronio o dal reato continuato loro ascritto perché il fatto non sussiste.
In particolare la Corte di merito precisava che il reato di appropriazione indebita non era stato nemmeno correttamente contestato perché in imputazione non si parlava della appropriazione di computer e comunque non sussisteva perché la copiatura di dati informatici non costituisce appropriazione indebita di una cosa mobile altrui, che, con riferimento al reato di cui all'articolo 615 ter c.p., non risultava che il sistema informatico fosse protetto da misure di sicurezza e, comunque, Caio e Sempronio in qualità di soci avevano il diritto di accedere ai dati informatici, e che per quel che concerne il reato di cui all'articolo 35 della legge 675 del 1996, norma abrogata dall'articolo 183 del decreto legislativo n. 196 del 2003, mancava il nocumento.
Avverso la decisione di secondo grado proponeva ricorso, evidentemente agli effetti civili ai sensi dell'articolo 576 c.p.p., soltanto la parte civile Tizio, che deduceva:
1) la manifesta illogicità della sentenza nella parte in cui la Corte di merito non ha ritenuto che fosse stata contestata l'appropriazione dei personal computers in dotazione dello studio e sui quali erano stati trasmessi i dati dei due servers dello studio, computers restituiti soltanto su richiesta del liquidatore;
2) la inosservanza ed erronea applicazione dell'articolo 646 c.p. nella parte in cui la sentenza impugnata ha ritenuto insussistente il fatto di appropriazione per essersi trattato di una attività di copia, sia perché l'appropriazione concerneva i due personal computers, sia perché la copia di documenti riservati per fini estranei a quelli della società costituiva appropriazione. A conforto della tesi il ricorrente citava due precedenti della Suprema Corte;
3) la manifesta illogicità della motivazione della sentenza impugnata nella parte in cui la Corte di merito aveva affermato che il sistema informatico non fosse protetto e nella parte in cui aveva affermato che i due imputati avessero titolo per introdursi e permanere nel sistema informatico stesso; il ricorrente ha ricordato che illogicamente la Corte di merito aveva fatto riferimento ai personal computers mentre la introduzione era avvenuta nei servers, che erano protetti e, comunque, il dato rilevante non sarebbe tanto la introduzione quanto la permanenza nel sistema al fine di estrarne copia e l'utilizzazione dei dati per fini estranei alla associazione;
4) la manifesta illogicità della motivazione nella parte in cui la Corte di merito asseriva l'insussistenza del delitto di cui all'articolo 167 del decreto legislativo n. 196 del 2003 per difetto di nocumento, nonostante avesse precedentemente riconosciuto il fatto che la condotta potesse essere posta a fondamento di pretesa risarcitoria a seguito di illecito civile.
Con memoria difensiva depositata il 23 giugno 2008 il ricorrente adduceva a sostegno dei motivi secondo e terzo del ricorso nuovi argomenti tratti dalla sentenza della IV Sezione della Corte di Cassazione 4 maggio 2006 - 14 settembre 2006 che aveva deciso su un caso analogo e che aveva qualificato il fatto della copiatura dei dati come truffa piuttosto che come appropriazione indebita.
I motivi posti a sostegno del ricorso proposto dalla parte civile Tizio sono fondati nei limiti di cui si dirà.
Deve essere in primo luogo esaminato il terzo motivo di impugnazione.
In effetti la decisione impugnata sul punto appare erronea e la motivazione che la sorregge illogica in più punti.
A Caio e Sempronio è stata contestata la violazione dell'articolo 615 ter c.p. perché, introdottisi nel sistema informatico dello Studio Tizio, si appropriavano dell'archivio informatico e procedevano al trattamento dei dati.
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 Tizio non ancora sciolto, effettivamente si introdussero nel sistema informatico dello studio costituito da due servers e da due

computers portatili, sui quali trasfusero 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.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

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.
Sul punto appare opportuno precisare che l'introdursi in un sistema informatico al fine di duplicare i dati ivi esistenti costituisce (come si chiarirà anche meglio in seguito) condotta tipica del delitto di cui all'articolo 615 ter c.p., perché la intrusione informatica può sostanziarsi sia in una semplice lettura dei dati contenuti nel sistema, sia nella copiatura degli stessi.
Orbene nel caso di specie è rimasto accertato, per come è lecito desumere dalla motivazione delle due sentenze di merito, che nei servers in questione erano custoditi i dati relativi ai clienti dello Studio Tizio, del quale il Tizio era non solo socio di maggioranza relativa, ma anche amministratore ed in quanto tale garante del corretto utilizzo degli strumenti esistenti nello studio, e, quindi, anche del sistema informatico, per le finalità tipiche dello studio associato.
È del tutto evidente che la copiatura dei dati, necessaria per fare funzionare lo studio concorrente creato dai due imputati, non era affatto compiuta nell'interesse dello Studio Tizio, ma al fine di avvantaggiare uno studio concorrente; da ciò è lecito desumere che detta copiatura sia avvenuta con il dissenso, in verità anche espresso perché mediante una guardia giurata il Tizio impedì, anche se successivamente alla consumazione dei fatti contestati, l'accesso ai locali dello studio al Caio ed al Sempronio, quanto meno tacito dell'amministratore dello studio che aveva il dovere di garantire il raggiungimento dei fini dello studio associato.
Cosicché appare priva di pregio la considerazione che i due imputati, in quanto ancora formalmente associati, avevano il diritto di accesso al sistema, perché il problema e, quindi, la violazione della norma consiste nel fatto che i due non avevano il diritto di accesso al fine di sottrarre dati importanti per lo studio associato, con i quali fare concorrenza allo stesso; tale attività costituisce certamente una indebita intrusione nel sistema informatico.
In dottrina, invero, è stato efficacemente rilevato che commette reato anche chi, dopo essere entrato legittimamente in un sistema, continui ad operare o a servirsi di esso oltre i limiti prefissati dal titolare e, quindi, in siffatta ipotesi ciò che si punisce è l'uso dell'elaboratore avvenuto con modalità non consentite più che l'accesso ad esso.
Gli argomenti esposti rendono evidente la erroneità della decisione impugnata, che non può, ovviamente, essere modificata per gli aspetti penali, mancando una impugnazione del Pubblico Ministero, ma che deve essere annullata agli effetti civili.
Per quanto concerne i motivi di ricorso primo e secondo, che riguardano il contestato delitto di appropriazione indebita, va detto che i pur pregevoli argomenti spesi dal ricorrente non possono essere accolti.
Ciò non tanto per le considerazioni dei giudici di appello sulla impossibilità di configurare il reato di cui all'articolo 646 c.p. quando l'appropriazione concerna beni immateriali, perché in tal caso l'appropriazione riguarderebbe, come correttamente osservato dal ricorrente, i due computers portatili, fatto che, contrariamente a quanto sostenuto dai giudici di appello, era stato debitamente contestato, ma per la semplice ragione che quelle indicate nel capo di imputazione non sono altro che le modalità attraverso le quali si è realizzata la intrusione nel sistema informatico punibile ai sensi dell'articolo 615 ter c.p.
Come si è già rilevato, infatti, la duplicazione dei dati contenuti in un sistema informatico costituisce condotta tipica del reato di cui all'articolo 615 ter c.p., potendo l'intrusione informatica punibile sostanziarsi sia in una semplice lettura dei dati contenuti nel sistema, sia nella copiatura degli stessi.
Ciò perché per accesso - così la rubrica dell'articolo 615 ter c.p. - deve ritenersi, come chiarito da autorevole dottrina, non tanto il semplice collegamento fisico, ovvero l'accensione dello schermo ecc., ma quello logico, ovvero il superamento della barriera di protezione del sistema che renda

possibile il dialogo con il medesimo in modo che l'agente venga a trovarsi nella condizione di conoscere dati, informazioni e programmi; la conoscenza dei dati, evidentemente, può avvenire sia con la semplice lettura, sia con la copiatura degli stessi.
Se quanto detto è vero deve ritenersi che quelle contestate non siano altro che semplici modalità per consumare il delitto di abusivo accesso informatico, cosicché la condotta del presunto delitto di appropriazione indebita si esaurisce in quella del delitto di cui all'articolo 615 ter c.p. Deve, pertanto, ritenersi che la condotta rubricata come ipotesi di violazione dell'articolo 646 c.p. rimanga assorbita dal reato di cui all'articolo 615 ter c.p. e non sia autonomamente punibile, trattandosi di modalità di consumazione di quest'ultimo delitto.
L'ultimo motivo di impugnazione è fondato.
In effetti l'unica ragione della esclusione del reato di cui all'articolo 167 del decreto legislativo n. 196 del 2003 - trattamento illecito dei dati - indicata dalla Corte di merito consiste nella ritenuta assenza del nocumento, dal momento che lo Studio Tizio continuò a funzionare anche dopo la illecita intrusione nel sistema informatico ed il trattamento dei dati illecitamente acquisiti.
In altra parte della motivazione, però, la Corte di merito aveva segnalato che non sussistevano i reati contestati, ma che non vi era dubbio che lo storno di clientela attuato tramite la acquisizione dei dati ed il trattamento degli stessi avesse prodotto dei danni che avrebbero potuto essere posti a fondamento di una pretesa risarcitoria a seguito di illecito civile.
Appare difficile conciliare una tale affermazione con la ritenuta assenza di nocumento, apparendo, peraltro, del tutto fuorviante l'argomento che lo studio aveva continuato a funzionare.
Il problema, infatti, non è questo perché nella specie potrebbe, a cagione delle condotte costituenti reato poste in essere da Caio e Sempronio, esservi stata una riduzione della attività e di ciò i giudici avrebbero dovuto tenere conto.
Insomma la motivazione posta a sostegno della assoluzione dal reato di cui all'articolo 167 del decreto legislativo 196 del 2003 è affetta da manifeste illogicità che impongono l'annullamento della sentenza impugnata anche se, come già detto, limitatamente agli effetti civili.
In conclusione per tutte le ragioni indicate la sentenza impugnata deve essere annullata agli effetti civili con rinvio al giudice civile competente per valore in grado di appello.
Le spese della parte civile vanno liquidate con la sentenza definitiva.

P.Q.M.

La Corte annulla agli effetti civili la sentenza impugnata con rinvio al giudice civile competente per valore in grado di appello.

*

Corte di Cassazione, Sez. VI penale, sent. 27 agosto 2002 n. 433
La Corte interviene in ordine alle fattispecie di cui all'art. 615 ter c.p. e 351 c.p.

Corte di Cassazione
Sez. VI penale, sent. 27 agosto 2002 n. 433

Fatto

Con ordinanza in data 23-30 agosto 2001, il Tribunale di Roma, adito ex articolo 309 c.p.p., riformava in parte, attraverso l'applicazione degli arresti domiciliari, l'ordinanza in data 6 agosto 2001 del Giudice per le indagini preliminari del medesimo Tribunale, con la quale era stata applicata a XX, funzionario del Ministero dell'Economia, la misura della custodia cautelare in carcere in ordine ai reati di cui agli articoli 81 cpv., 110, 615-ter, commi primo, secondo n.2, e terzo, e 61 n.2 c.p. (capo 2: commesso in Roma dal 18 dicembre 2000 al febbraio 2001) e di cui agli articoli 110, 351 c.p. (capo 3: commesso in Roma in data successiva e prossima al 18 dicembre

2000).
Più dettagliatamente, al XX veniva contestato, quanto al capo 2, in concorso con YY, tenente colonnello dei Carabinieri, ZZ, brigadiere CC. del Nucleo Radiomobile di …, e OO, maresciallo CC. del ROS, sezione Anticrimine di …, di essersi introdotto abusivamente nel sistema informatico della sezione ROS di … delegata allo svolgimento delle indagini nel procedimento numero … e in varie banche-dati interforza; e quanto al capo 3, in concorso con i predetti soggetti, di avere sottratto la trascrizione del verbale di interrogatorio reso da PPP. nel procedimento numero … cosa particolarmente custodita nella sezione ROS CC. di …, delegata allo svolgimento delle indagini e custode del documento.
Avverso la riferita ordinanza del Tribunale del Riesame di … ricorre per Cassazione il XX, a mezzo dei difensori, che deducono:
1) Manifesta illogicità della motivazione in punto di sussistenza dei gravi indizi di colpevolezza, posto che il Tribunale, trascurando le puntuali deduzioni difensive, si è basato su una mera presunzione (l'interesse del XX a conoscere il contenuto dell'interrogatorio del PPP) per desumerne una sua condotta di istigazione nei confronti di coloro che materialmente appresero copia della trascrizione del predetto atto difensivo; essendo invece da ritenere che il semplice movente costituisce un mero indizio, non idoneo a sorreggere una misura cautelare, in mancanza di altri elementi indiziari. In particolare il Tribunale ha trascurato di considerare che il XX poteva legittimamente ottenere copia delle trascrizioni dell'interrogatorio reso dal PP; che tale atto riguardava una moltitudine di persone potenzialmente interessate a ottenerne copia; che coloro che materialmente si procurarono abusivamente copia dell'interrogatorio non necessariamente erano stati istigati da chi aveva interessa a conoscerne il contenuto, potendo ben avere agito a sua insaputa, per compiacerlo o addirittura per scopo intimidatorio.
2) Erronea applicazione dell'articolo 351 c.p., atteso che l'acquisizione di una mera copia di un atto (nella specie, attraverso la stampa del relativo documento informatico) non determina la sottrazione o la dispersione di questo, che rimane comunque nella disponibilità del pubblico ufficio.
3) Mancanza di motivazione in ordine alle esigenze cautelari, essendosi omesso di esporre quali specifiche esigenze imponessero l'adozione della misura custodiale, sia pure nella forma domiciliare.

Diritto

Il primo motivo di ricorso, al limite dell'ammissibilità, appare infondato. Contrariamente a quanto dedotto, il Tribunale non ha tratto gli indizi di colpevolezza in ordine al reato di cui al capo 2 da mere presunzioni, avendo fondato il suo convincimento non solo sul movente rappresentato dall'evidente interesse dell'indagato a conoscere il contenuto dell'interrogatorio del PPP ma sulle specifiche ed obiettive risultanze delle intercettazioni di comunicazioni intercorse tra il XX, il YY e il OO, in ordine alle quali il ricorrente non spende parola.
In ordine al terzo motivo di ricorso deve rilevarsi la sopravvenuta perdita di interesse, essendo stato nel frattempo il XX. posto in libertà con successivo provvedimento.
E' invece fondato il secondo motivo.
La fattispecie incriminatrice di cui all'articolo 351 c.p. prevede la condotta di chi "sottrae, sopprime, distrugge, disperde o deteriora corpi di reato, documenti ovvero un'altra cosa mobile particolarmente custodita in un pubblico ufficio, o presso un pubblico ufficiale o un impiegato che presti un pubblico servizio".
Nel caso in esame è stato contestato al XX di avere in concorso con i coindagati, sottratto la trascrizione del verbale di interrogatorio reso da PPP nel procedimento penale n. …, cosa particolarmente custodita nella sezione ROS dei CC. di …, delegata allo svolgimento delle indagini e custode del documento.

Tale condotta sarebbe stata realizzata attraverso l'ottenimento della stampa dell'atto predetto versato sull'archivio informatico del ROS.
Ora, benché la condotta presa in esame dalla norma incriminatrice non esclude che essa possa riguardare non solo l'originale di un atto, ma anche una copia di esso, che rilevi per la sua individualità (Cass., sez. VI, 16 marzo 1993, Chirico), il concetto stesso di sottrazione implica che una determinata res fuoriesca dalla sfera di disponibilità del legittimo detentore, che ne venga conseguentemente privato; il che nella specie non si è verificato, in quanto l'ufficio del ROS non è stato affatto privato dell'atto e nemmeno di una sua copia, trattandosi di una riproduzione su carta, teoricamente illimitata, di un file esistente su supporto informatico, rimasto intatto. In altri termini, la "copia" dell'atto non preesisteva fisicamente alla condotta di impossessamento, ma è stata ottenuta proprio tramite l'abusiva stampa del file, sicché non può dirsi che l'atto sia stato "sottratto" al pubblico ufficio, ferma restando la configurabilità del distinto reato di cui all'articolo 615-ter c.p.
L'ordinanza impugnata va pertanto annullata senza rinvio, limitatamente al reato di cui all'articolo 351 c.p., mentre il ricorso va rigettato nel resto.

P.Q.M.

Annulla senza rinvio l'impugnata ordinanza limitatamente al reato di cui all'articolo 351 c.p. Rigetta nel resto il ricorso.
Così deciso addì 19 febbraio 2002.
Il Consigliere Estensore
Il Presidente
Depositato in Cancelleria VI Sezione Penale
Oggi, 27 agosto 2002

*

Tribunale di Torino, Sent. del 30 settembre 2002

Ricariche carte telefoniche, non è configurabile l'ipotesi di accesso abusivo al sistema informatico di cui all'art. 615 quater. c.p. né quella di frode informatica di cui all'art. 640 ter c.p.

*

Cass. Pen., Sent. 7 Nov - 6 Dic. 2000 n. 1675

Accesso abusivo: deve ritenersi che, ai fini della configurabilità del delitto, assuma 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, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi.

Corte di Cassazione,
Sent. 7 Nov - 6 Dic. 2000 n. 1675

Motivi della decisione

1. Con la sentenza impugnata la Corte di Appello di Torino confermò la dichiarazione di colpevolezza di XX. e di YY in ordine al delitto di accesso abusivo al sistema informatico della TT s.r.l., gestrice di contabilità per conto terzi, e dichiarò colpevole del medesimo reato, quale autore materiale dei fatti, il programmatore OO., che in primo grado ne era stato assolto per difetto di dolo.
Risulta dalle sentenze di merito che XX., già socio di RR. nella TT., nel 1994 era uscito dalla società per intraprendere analoga attività con il commercialista YY., già collaboratore esterno della TT., e, non avendo ottenuto di poter utilizzare come locatario l'impianto informatico della società, ne aveva copiato i dati su un analogo calcolatore con l'aiuto di OO., facilitandosi così l'acquisizione di un gran numero di clienti della TT.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

Ricorrono per Cassazione gli imputati, che hanno proposto cinque motivi di impugnazione.
Con il primo motivo i ricorrenti lamentano mancanza di motivazione sul motivo di appello con il quale era stato dedotto che OO. e il suo datore di lavoro AA., proprietario del programma concesso in uso sia alla TT. sia a XX. e YY, avevano diritto di copiare e modificare il software. E con il connesso terzo motivo si lamenta che i giudici d'appello abbiano omesso di considerare il fatto, ben valorizzato invece dal tribunale, che OO. agiva su disposizione di AA. e non aveva motivo di dubitare della legittimità di tali disposizioni anche con riferimento alle copie effettuate in favore di XX. e YY.
Con il secondo motivo i ricorrenti deducono violazione dell'art. 615 *ter* c.p., lamentando che i giudici del merito abbiano ritenuto configurabile il reato contestato anche in mancanza di protezioni di sicurezza interne al sistema, mentre la dottrina è concorde nell'escludere la rilevanza di protezioni esterne.
Con il quarto motivo i ricorrenti deducono mancanza di motivazione in ordine alla determinazione della pena, irrogata in misura identica a tutti gli imputati, senza alcuna considerazione per le diverse posizioni soggettive.
Con il quinto motivo infine i ricorrenti deducono violazione dell'art. 538 comma 1 c.p.p., lamentando che i giudici del merito si siano pronunciati su una domanda in realtà non proposta dalla parte civile TT., che, costituitasi per il reato di cui all'art. 640 *ter* c.p. originariamente contestato, non aveva rinnovato la costituzione anche per il reato di cui all'art. 615 *ter* c.p., contestato in udienza.
I motivi del ricorso sono stati successivamente illustrati con ampia memoria depositata il 10 giugno 2000.
Una memoria è stata altresì depositata dalla parte civile.
2.Il ricorso deve essere rigettato.
Il primo motivo del ricorso, come il motivo d'appello cui si riferisce per lamentarne l'immotivato rigetto, non distingue tra il programma informatico, di cui si assume fosse proprietario AA., e i dati informatici, che erano certamente nell'esclusiva disponibilità della TT. Ma l'ipotesi di d'accusa di cui si discute presuppone proprio quella distinzione, perché la parte civile si lamenta di un accesso abusivo finalizzato alla riproduzione dei dati informatici, non del software. Sicché era manifestamente infondato il motivo d'appello con il quale si deduceva l'inesistenza del reato in relazione al diritto di TT., del proprietario del programma, di copiarlo e aggiornarlo. E secondo una consolidata giurisprudenza di questa Corte, deve essere considerato privo di fondamento il motivo del ricorso per cassazione con il quale si deduca mancanza di motivazione in ordine a un motivo d'appello inammissibile o manifestamente infondato (Cass. Sez. I, 23/3/87, Imbimbo, n. 176707; Sez. I, 28/9/87, Ciusco, m. 177007; Cass. Sez. IV, 26/9/90, Pilloni, m. 185682; Cass. Sez. I, 5/3/91, Calò, m. 186972; Cass. Sez. V, 18/2/92, Cremonini, m. 189818; Cass. Sez. I, 28/3/96, Bruno, m. 204548).
Ne consegue anche l'inammissibilità, per violazione dell'art. 606 comma 3 c.p.p., del terzo motivo del ricorso, con il quale si lamenta l'erronea affermazione della responsabilità di V. B., perché una volta chiarita la distinzione tra i dati informatici e il programma destinato a elaborarli, la censura rimane riferibile a una mera valutazione di merito circa la consapevolezza da parte dell'imputato di una tale distinzione e della conseguente illiceità della copia dei dati.
Il secondo motivo del ricorso pone il problema della natura della protezione di sicurezza rilevante ai fini della configurabilità del delitto previsto dall'art. 615 *ter* c.p.
La corte di appello ha ritenuto che, ai fini della configurabilità del reato, assumano rilevanza non solo le protezioni interne al sistema informatico, come le chiavi d'accesso, ma anche le protezioni esterne, come la custodia degli impianti, in particolare quando, come nel caso in esame, si tratti di banche dati private, per definizione interdette a coloro che sono estranei all'impresa che le gestisce.

I ricorrenti sostengono, invece, che soltanto la protezione interna al sistema è idonea a manifestare la volontà del proprietario di escludere terzi, come dimostrerebbe il fatto che il D.P.R. n. 318 del 1999 richiede come necessaria una chiave d'accesso nel trattamento dei dati personali.
Il motivo di ricorse è infondato.
L'art. 615 *ter* comma 1 c.p. punisce non solo chi s'introduce abusivamente in un sistema informatico o telematico ma anche chi "vi si mantiene contro la volontà esplicita o tacita di chi ha il diritto di escluderlo". Ne consegue che la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sé, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone.
Non si tratta perciò di un illecito caratterizzato dall'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio, che è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un "domicilio informatico".
Certo è necessario che l'accesso al sistema informatico non sia aperto a tutti, come talora avviene soprattutto quando si tratti di sistemi telematici. Ma deve ritenersi che, ai fini della configurabilità del delitto, assuma 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, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi. Ed è certamente corretta, in questa prospettiva, la distinzione operata dalla corte d'appello 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. 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'acceso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva. Sicché correttamente i giudici del merito hanno ritenuto configurabile il reato nella condotta di OO., che, autorizzato all'accesso per controllare la funzionalità del programma informatico, si avvalse dell'autorizzazione per copiare i dati da quel programma gestiti.
Privo di qualsiasi pertinenza al caso in esame è, infine, il "regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15 comma 3 della L. 31/12/96, n. 675". Infatti la mancata adozione delle misure minime di sicurezza nel trattamento di dati personali è prevista come reato dall'art. 36 della L. 675/96; ma evidentemente la consumazione di questo reato non esime, comunque, da responsabilità chi violi i pur insufficienti meccanismi di protezione esistenti.
Il quarto motivo del ricorso è inammissibile per violazione dell'art. 606 comma 3 c.p.p., perché propone censure attinenti al merito della decisione impugnata, congruamente giustificata con riferimento alla ritenuta gravità della violazione del rapporto fiduciario con la parte lesa, comune a tutti gli imputati.
Come s'è detto, con il quinto motivo i ricorrenti deducono violazione dell'art. 538 c.p.p., lamentando che i giudici del merito si siano pronunciati su una domanda di risarcimento danni non proposta dalla parte civile per il reato di cui all'art. 615 *ter* c.p., contestato in udienza. Tuttavia gli stessi ricorrenti riconoscono che, sin dal primo grado del giudizio, la parte civile concluse

chiedendo la condanna degli imputati al risarcimento anche dei danni derivanti dal reato previsto dall'art. 615 *ter* c.p. ; sicché non si può dire che i giudici del merito si siano pronunciati su una domanda non proposta.
In realtà i ricorrenti pongono una questione diversa da quella formalmente enunciata, perché essi lamentano che per il nuovo reato contestato in udienza non vi era stata costituzione di parte civile; e sostengono che una tale rinnovata costituzione sarebbe stata invece necessaria, secondo quanto previsto anche dalla sentenza n. 98 del 1996 della Corte Costituzionale. Sennonché la giurisprudenza di questa Corte, richiamata anche dalla Corte Costituzionale, ha ben chiarito che occorre distinguere tra la posizione della persona offesa non costituita, che in caso di nuove contestazioni ha diritto alla sospensione del dibattimento onde potersi eventualmente costituire parte civile per la nuova udienza, e il caso della persona offesa già costituita parte civile, che ha un analogo diritto, ma solo "in vista della possibile modifica, sotto il profilo tanto della *causa petendi* quanto del *petitum*, del già costituito rapporto processuale" (Cass. Sez. III, 23/9/95, Roncati). Sicché, per la parte civile già costituita non occorre rinnovare la costituzione in relazione al nuovo reato contestato in udienza all'imputato, ma è sufficiente modificare la domanda già proposta. E nel caso in esame deve ritenersi che un idoneo aggiornamento della domanda si ebbe appunto con la formulazione delle conclusioni in chiusura del dibattimento di primo grado.
Il ricorso va pertanto rigettato.

P.Q.M.

La Corte rigetta il ricorso e condanna i ricorrenti in solido al pagamento delle spese di procedimento e inoltre al rimborso delle spese in favore della parte civile, liquidate in complessive L. 2.306.000, di cui L. 2.000.000 per onorari.
Roma, 7 novembre 2000
Il Presidente
Il consigliere relatore (dr. Aniello Nappi)
Depositato in cancelleria Addì 6 dicembre 2000

*

Tribunale penale di Roma, Uff. GIP, sent. 21 aprile 2000 n. 6677/99

Pronuncia del GIP di Roma in ordine ad uno dei primi fatti approdati alla decisione di un Tribunale in merito alla fattispecie in questione. E' molto utile verificare la tesi in forza della quale la mancata idoneità della misura di sicurezza venga posta a fondamento di una pronuncia di assoluzione per carenza dell'elemento oggettivo. Tesi successivamente disattesa dalla Cassazione, in ordine però ad episodi e fatti differenti.

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
Il Giudice dell'udienza preliminare dr. E.L. all'udienza del 4.4.2000 ha pronunciato e pubblicato mediante lettura del dispositivo la seguente

SENTENZA

nei confronti di XX **i**mputato del reato di cui all'art. 615 ter, 2° e 3° comma c.p., per essersi introdotto abusivamente nel sito telematico del G.R.1, rinominando con lo stesso nome di quello autentico e sostituendo il file contenente il Radio Giornale delle ore 13.00, con un altro file contenente una serie di critiche alla Società YY. e al nuovo sistema operativo denominato …
Con l'aggravante di essersi inserito in un sistema telematico di pubblico interesse.
Fatto accaduto in Roma il 10.07.1998, dalle ore 17.30 alle ore 17,53 circa.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

PREMESSA

Il P.M. chiedeva, con atto depositato l'1.6.1999, il rinvio a giudizio di XX. per il reato di cui in rubrica.

Si svolgeva quattro udienze preliminari finalizzate anche all'ammissione della perizia tecnica, con le formalità dell'incidente probatorio.

All'esito dell'udienza del 4.4.2000 il P.M. chiedeva il rinvio a giudizio e la difesa di proscioglimento dell'imputato.

MOTIVAZIONE

Dagli atti delle indagini preliminari (in particolare verbale di interrogatorio dell'indagato e verbale di sommarie informazioni rese dal dipendente Rai OO) risulta che l'imputato in data 10.7.1998, utilizzando dalla sua abitazione un computer (Pentium II con velocità 266 Mhz e con Mbyte 64 di memoria principale), dotato di sistema operativo Windows 95, collegato ad Internet attraverso connessione telefonica con il nodo di Ancona del fornitore di servizi Internet TIN e servendosi dell'account dell'utente "xxxxxx" (attribuito dalla TIN a XXXXXXX di Mantova e che risulterà poi nei file log della RAI), si introduceva nel sito telematico del G.R.1, sostituendo il file contenente il radio Giornale delle ore 13.00 con altro file di sua creazione, contenente una serie di critiche alla Società YY e al sistema operativo …

Della predetta manomissione la redazione si accorgeva soltanto dopo due giorni per effetto delle e/mail inviate da due utenti.

Appresa dalla stampa la notizia della denuncia presentata dalla Rai contro ignoti, il XX tempestivamente e spontaneamente dichiarava di essere l'autore del fatto attraverso una e/mail (foglio 83) inviata alla testata giornalistica La Repubblica, il cui testo si trascrive: "sono entrato nel server mm1.rai.it grazie a una password fregata al pc di OO, che, molto imprudentemente, ha il proprio disco fisso in condivisione e dunque è accessibile liberamente all'esterno". Tali affermazioni ripeteva sostanzialmente in sede di spontanee dichiarazioni rese alla P.G., in sede di interrogatorio delegato alla P.G. ex art. 370 c.p.p., nonché avanti al perito. In particolare nell'interrogatorio precisava di non avere agito con l'intenzione di arrecare danni al sistema della Rai e mostrava di essere sinceramente pentito.

In sintesi l'imputato ha sostenuto che, usando un programma per la ricerca di computer su Internet con condivisioni aperte, è riuscito ad accedere senza problemi al computer della Rai denominato GRR4. Durante questo accesso l'imputato ha affermato di aver trovato nel "direttorio" principale dell'hard disk un file che citava la macchina denominata MM1, che costituiva il server della Rai contenente i file real audio con i Radio Giornali accessibili da Internet. Questo stesso file citava inoltre l'account "xxx", utilizzato dai dipendenti Rai per accedere al computer MM1 ed il programma ws ftp, utilizzato per trasferire su quest'ultimo computer i file audio prodotti su altre macchine. Ha così effettuato una connessione diretta al server MM1 con l'account "xxx" e, utilizzando sul suo computer, il programma ws ftp, ha ridenominato il file gr1-1007.ra, contenente il Radio Giornale delle ore 13.00 del 10.7.98, senza cancellarlo. Con tale programma ha infine memorizzato su MM1 un nuovo file denominato gr1-1007.ra da lui preparato contenente le critiche al … In tal modo l'utente che accedeva al sito Internet della Rai riceveva questo ultimo file in risposta alla richiesta del radio Giornale delle ore 13.00.

La perizia, espletata nelle forme dell'incidente probatorio, ha chiarito che l'imputato ha sfruttato una caratteristica tipica dei computer dotati di sistema operativo Windows 95 e collegati ad Internet. Se su questi computer risulta attivo il servizio condivisione file e stampanti su protocollo Netbios e non si definisce una password, si rendono direttamente accessibili i file anche a tutte le macchine con analogo sistema operativo Windows 95 connesse su Internet: in tal modo è possibile dare ad altri utenti della rete la visibilità dei propri dati. Il computer della Rai GRR4, per l'appunto, aveva attivata la condivisione risorse.

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

Il perito ha inoltre verificato la validità della procedura tecnica utilizzata dall'imputato ed in particolare ha testato una versione dei programmi (fornitigli dallo stesso XX) per la ricerca di computer su Internet con condivisioni aperte. Ha così escluso che, soddisfatte le condizioni anzidette, l'iter seguito richiedesse la conoscenza di elementi forniti da terzi.
Ciò posto va verificata la corrispondenza del fatto penalmente rilevante ascritto all'imputato con la fattispecie incriminatrice di cui all'art. 615 ter comma 2 e comma 3 c.p.
Nonostante la generica formulazione del capo di accusa si ritiene che il p.m. abbia inteso contestare al XX la condotta dell'accesso abusivo a sistema informatico di pubblico interesse (comma 3), protetto da misure di sicurezza, determinando l'interruzione del suo funzionamento (comma 2 n. 3).
La condotta materiale tenuta dall'agente, consistente nella sua introduzione nel sistema della Rai con sostituzione del file contenente il radio Giornale con altro contenente critiche alla società YY, è inquadrabile nella fattispecie aggravata suddetta. Tuttavia non risultano elementi di prova sufficienti a dimostrare l'esistenza di misure di sicurezza idonee a proteggere il sistema violato. A tale proposito si osserva che il legislatore con l'introduzione della norma incriminatrice di cui all'art. 615 ter ha inteso tutelare non la privacy di qualsiasi "domicilio informatico", ma soltanto quella di sistemi "protetti" contro il pericolo di accessi da parte di persone non autorizzate.
Nel caso specifico nella relazione il perito ha sottolineato che il sistema informatico della Rai era configurato in modo tale da non essere completamente sicuro: esisteva un computer (GRR4) che consentiva l'accesso agli estranei tramite rete (secondo quanto suesposto) e che conteneva al suo interno la password per l'accesso al computer server (MM1) manomesso. Aggiunge che sebbene la macchina GRR4 risultava protetta da firewall, cioè da un sistema di controllo del traffico di dati sulla rete locale, probabilmente tale firewall non era idoneo. Ciò potrebbe essere dipeso dal fatto che, avendo il GRR4 due connessioni esterne (una alla rete locale ed una direttamente ad Internet), il firewall verificava solo il transito dei dati attraverso una delle due connessioni oppure non era ben configurato (in particolare non controllava i servizi offerti dal processo Netbios: p. 5 della relazione peritale).
All'udienza del 4.4.2000 il perito ha dichiarato che "il personale Rai ha confermato che esisteva un computer con due tipi di connessione, una delle quali non era sufficientemente protetta".
Sulla base delle risultanze dell'elaborato peritale si ritiene non sufficientemente provata l'idoneità delle misure di sicurezza predisposte dalla Rai a tutela del proprio sistema informatico.
Del resto è ormai acclarato che i tradizionali mezzi di protezione software, in particolare quelli incentrati sulle c.d. chiavi di accesso non offrono certezza assoluta di impenetrabilità, essendo la loro individuazione soltanto una questione di tempo e livello tecnologico. Inoltre nel caso specifico la password del computer MM1 era citata in un file contenuto in una macchina (GRR4) vulnerabile.
Considerato che l'esistenza di mezzi efficaci di protezione è elemento costitutivo della fattispecie incriminatrice di cui all'art. 615 ter c.p., deve dichiararsi il non luogo a procedere con la formula di cui all'art. 425 comma 3 c.p.p., anche perché atteso il tempo trascorso e considerato che la Rai ha sostituito le precedenti misure di sicurezza con altre (come riferito dal perito in udienza), è del tutto improbabile che ulteriori indagini possano evolvere in senso favorevole all'accusa.

p.q.m.

visto l'art. 425 comma 3 c.p.p.: dichiara il non luogo a procedere nei confronti di XX. in relazione all'imputazione di cui alla rubrica, perché il fatto non sussiste.
Roma, 4.4.2000
Il giudice dr. E. L.
Depositato in Cancelleria Oggi, 21.4.2000

*

Cass. Pen., Sent. n. 3067 del 1999

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.

Definizione di sistema informatico o telematico secondo la giurisprudenza.

Per sistema informatico o telematico, secondo la Cassazione deve intendersi "un complesso 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 un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente"

Indicazioni: in questo documento vengono raccolte le principali massime (o pronunce per esteso) inerenti il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p. Le sentenze sono citate in ordine cronologico, procedendo dalla più recente. La raccolta non è esaustiva. Le pronunce sono state rese anonime. Per i testi originali si raccomanda di consultare il sito della Cassazione, declinando per eventuali errori od omissioni.