Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema".

REPUBBLICA ITALIANA

In nome del Popolo Italiano
LA CORTE SUPREMA DI CASSAZIONE
SEZIONI UNITE PENALI

Composta da
Ernesto Lupo - Presidente -
Nicola Milo
Maria Cristina Siotto
Aldo Fiale - Relatore -
Ruggero Galbiati
Giovanni Conti
Franco Fiandanese
Maurizio Fumo
Alberto Macchia
ha pronunciato la seguente

SENTENZA

sui ricorsi proposti da

1. C. G., nato a Roma il 20/06/1968
2. S. G., nato a Roma il 13/07/1964
3. T. A., nata a Roma il 23/09/1964

avverso la sentenza del 19/05/2009 della Corte di appello di Roma
visti gli atti, la sentenza impugnata e i ricorsi;
udita la relazione svolta dal consigliere Aldo Fiale;
udito il Pubblico Ministero, in persona del Procuratore Generale Aggiunto Gianfranco Ciani, che ha concluso chiedendo l'annullamento con rinvio della sentenza impugnata, nei confronti del S., limitatamente al mancato giudizio di bilanciamento delle circostanze nei trattamento sanzionatorio; e per ilrigetto dei ricorsi del C. e della T.;
udito l'avv. Urbano Del Balzo, per la parte civile C. M., che ha concluso chiedendo il rigetto dei ricorsi;
uditi i difensori dei ricorrenti avvocati Alessandro Vannucci, per C. e T., e Fabrizio Merluzzi, per S., che hanno concluso chiedendo l'accoglimento dei rispettivi ricorsi.

RITENUTO IN FATTO

1. La Corte di appello di Roma, con sentenza del 19 maggio 2009, in parziale riforma della sentenza emessa il 16 ottobre 2007, all'esito di giudizio abbreviato, dal Giudice della udienza preliminare del Tribunale in sede:
a) ribadiva l'affermazione della responsabilità penaledi:
G. S. in ordine al delitto di cui agli artt. 81, comma secondo, e 615-ter, comma secondo, n. 1, e comma terzo, cod. pen., perché, quale maresciallo in servizio presso la stazione dei Carabinieri di Roma-Flaminio, con più azioni esecutive di un medesimo disegno criminoso, abusivamente si introduceva nel sistema informatico denominato S.D.I. (Sistema di Indagine), in dotazione alle forze di polizia, sistema protetto da misure dì sicurezza, con abuso dei poteri e violazione dei doveri inerenti la funzione di ufficiale di p.g. e con violazione delle direttive concernenti l'accesso allo S.D.I. da parte di appartenenti alle forze dell'ordine e all'Arma dei Carabinieri: in particolare, accedendo a tale sistema informatico nonostante fosse fuori dal servizio e, comunque, non dovesse svolgere alcuna indagine sul conto di C. M. ed A. T., si impossessava di notizie afferenti la sfera privata e le vicende giudiziarie di entrambi, nonché di altre otto persone legate a vario titolo al M. (in Roma, il 13 giugno 2006);
G. S., G. C. ed A. T. in ordine al delitto di cui all'art. 326 cod. pen., perché: il S., violando i doveri inerenti la sua funzione e comunque abusando della sua qualità,

rilevava al C. le notizie di ufficio, illecitamente acquisite e che dovevano rimanere segrete o riservate, riguardanti C. M. e A. T.; il C., venuto in possesso dei documenti contenenti le anzidette notizie di ufficio sul conto del M., coniuge separato della T., sua convivente, li consegnava alla donna al fine di procurarle un ingiusto profitto e comunque di arrecare al M. un danno ingiusto; la T., al fine di procurarsi un ingiusto profitto e comunque di arrecare al coniuge separato un danno ingiusto, inviava per posta al M. i tabulati dell'interrogazione al S.D.I.;
b) determinava le pene, con le già riconosciute circostanze attenuanti generiche, in un anno e otto mesi di reclusione per il S. ed in dieci mesi di reclusione per ciascuno degli altri due imputati, confermando la concessione dei doppi benefici di legge al S. ed alla T.;
c) confermava le statuizioni risarcitone in favore del M., costituitosi parte civile.
2. Secondo la ricostruzione dei fatti operata dai giudici dei mento, il S. si era introdotto nel sistema informatico S.D.I., protetto da misure di sicurezza e relativo all'ordine pubblico e alla sicurezza pubblica, usando il proprio codice di identificazione per finalità diverse da quelle che gli consentivano l'accesso: precisamente, per compiere accertamenti su C. M. (coniuge separato della T., divenuta successivamente convivente del C.), non per ragioni di ufficio, bensì a seguito della richiesta a lui rivolta dal C., per motivi personali ricollegabili ai contrasti tra la T. e il M. nel procedimento di separazione in corso.
Il S. aveva quindi acquisito una serie di informative relative alla persona del M. ed ai procedimenti penali in cui quello era coinvolto e le aveva consegnate ai C., *che,* insieme alla T., aveva spedito la documentazione più imbarazzante al M., con la scritta *"io so",* quale elemento di pressione ed fini del procedimento di separazione.
Quanto alla qualificazione giuridica del fatto ascritto al S., la Corte di appello specificava di condividere l'orientamento espresso dalla Corte di cassazione, Sez. 5, n. 1727 del 30/09/2008, dep. 2009, Romano, secondo il quale l'ipotesi di reato prevista dall'art. 615-ter, comma secondo, n. 1, cod. pen., sanziona anche la condotta del pubblico ufficiale che, pure essendo specificamente abilitato a consultare il sistema informatico, vi abbia però fatto accesso «con abuso dei poteri o con violazione dei doveri inerenti la funzione o il servizio [...] o con abuso della qualità di operatore del sistema».
3. Avverso la suddetta sentenza hanno proposto separati ricorsi per cassazione il C. e la T., i quali, con doglianze sostanzialmente comuni, hanno dedotto violazione dì legge e difetto di motivazione in relazione ai delitto di rivelazione di segreti di ufficio (art. 326 cod. pen.) ad essi ascritto, che resterebbe escluso dalla pregressa conoscenza delle vicende giudiziarie del M. da parte di quest'ultimo e della T. (la quale le aveva apprese nel corso della convivenza matrimoniale), tenuto conto dell'orientamento della giurisprudenza di legittimità secondo cui presupposto della condotta illecita è che il destinatario della rivelazione non conosca già l'oggetto della stessa. In caso contrario, si verterebbe in ipotesi di reato impossibile, in quanto non si può "rivelare" una notizia a chi già la conosca.
Nella specie, inoltre, non sarebbe configurabile la causazione di alcun nocumento agli interessi tutelati a mezzo della notizia da tenere segreta.
4. Anche il S. ha proposto ricorso, deducendo i seguenti motivi:
a) erronea applicazione dell'art. 599, comma 2, cod. proc. pen., con conseguente nullità del giudizio e della successiva sentenza, a causa dell'illegittimo diniego del differimento dell'udienza nel giudizio di appello, chiesto per infermità del ricorrente documentata da certificato medico, che sarebbe stato disatteso dalla Corte di appello senza esplicitazione delle ragioni per cui la malattia non sarebbe stata idonea a legittimare l'impedimento dell'imputato;
b) erronea interpretazione dell'art. 615-ter cod. pen., nonché mancanza e manifesta illogicità della motivazione in ordine alla sussistenza del reato di accesso abusivo a un sistema informatico.
Si prospetta, sui punto, che la Corte territoriale erroneamente avrebbe attribuito un duplice e diverso significato al sintagma *"accesso abusivo",* a seconda che si versi nel primo ovvero nel secondo comma della norma incriminatrice in oggetto.
Le condotte indicate nel secondo comma, n. 1, dell'art. 615-ter cod. pen. non integrane fattispecie delittuose distinte ed autonome rispetto a quelle descritte nel primo comma,

costituendo invece ipotesi aggravate finalizzate ad innalzare la sanzione da applicare a quei soggetti *che* in ragione della loro funzione - e purché non legittimati *ab initio* - sono facilitali ad attingere informazioni sensibili;
c) mancanza, illogicità e manifesta contraddittorietà della motivazione in ordine al reato di cui all'art.. 326, comma secondo, cod. pen., rilevandosi una frattura logica nel ragionamento volto a riconnettere all'interesse del C. ad avere determinate informazioni la prova certa di una condotta dolosa (invece che colposa) del S. al momento della diffusione delle stesse informazioni;
d) manifesta illogicità del trattamento sanzionatorio, posto che la Corte di appello ha limitato l'efficacia delle riconosciute attenuanti generiche e operato un consistente aumento a titolo di continuazione in ragione di un tornaconto personale del S., che risulta meramente affermato a fronte dell'esclusione di ogni interesse economico del medesimo soggetto.
5. Il ricorso è stato assegnato alla Quinta Sezione penale, la quale, all'udienza dell'11 febbraio 2011 (**con ordinanza depositata il 23 marzo 2011**), ha rilevato che il punto nodale della vicenda processuale in esame è costituito dalla qualificazione giuridica della condotta posta in essere dal maresciallo dei carabinieri Sentili' con le modalità dianzi enunciate.
Si osserva che la Corte di appello ha ritenuto che la suddetta condotta integri il reato sanzionato dall'art. 615-ter cod. pen., dichiarando di aderire all'orientamento espresso dalla giurisprudenza di legittimità con la citata sentenza Romano.
Detto orientamento era stato già espresso dalla stessa Quinta Sezione con la **sentenza n. 12732 del 07/11/2000, Zara**, ove era stato argomentato che *«l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa* [prevista dall'art. 615-ter cod. pen.] *anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva».*
In tale prospettiva ermeneutica, la norma posta dall'art. 615-ter cod. pen., nel configurare il reato di "accesso abusivo", sanziona non solo la condotta del cosiddetto *hacker* o "pirata informatico", cioè di quell'agente che, non essendo abilitato ad accedere al sistema protetto, riesca tuttavia ad entrarvi scavalcando la protezione costituita da una chiave di accesso *(password),* ma anche quella del soggetto abilitato all'accesso, e perciò titolare di un codice d'ingresso, che s'introduca legittimamente nel sistema, per finalità però diverse da quelle delimitate specificamente dalla sua funzione e dagli scopi per i quali la *password* gli è stata assegnata.
L'enunciata interpretazione era stata ribadita, sempre dalla Quinta Sezione, con le sentenze: **n. 37322 del 08/07/2008, Bassani**, n. 1727 del 30/09/2008, Romano, n. 13006 del 13/02/2009, Russo, n. 2987 del 10/12/ 2009, Matassich, n. 19463 dei 16/02/2010, Jovanovic, n. 39620 del 22/09/2010, Lesce.
In particolare, nelle sentenze Bassani e Lesce, era stato espressamente enunciato che il primo comma dell'art. 615-ter cod. pen. sanziona non soltanto l'introduzione abusiva in un sistema informatico protetto, ma anche il mantenersi al suo interno - contro la volontà espressa o tacita di chi abbia il diritto di escluderlo - da parte di soggetto abilitato, il cui accesso, di per sé legittimo, diviene abusivo, e perciò illecito, per il suo protrarsi all'interno del sistema per fini e ragioni estranee *a* quelle d'istituto.
Un orientamento diverso e contrastante era stato espresso, invece, dalle sentenze Migliazzo (Sez. 5, n. 2534 del 20/12/2007), Scimia (Sez. 5, n. 26797 del 29/05/2008), Peparaio (Sez. 6, n. 3290 del 08/10/2008), **Genchi (Sez. 5, n. 40078 *del* 25/06/2009)**, che avevano valorizzato il dettato della prima parte del primo comma dell'art. 615-ter cod. pen., e avevano ritenuto perciò illecito il solo accesso abusivo, e cioè quello effettuato da soggetto non abilitato, mentre sempre e comunque lecito consideravano l'accesso del soggetto abilitato, ancorché effettuato per finalità estranee a quelle d'ufficio (espressamente sul punto la sentenza Peparaio) e perfino illecite (cosi la sentenza Scimia).
6. A fronte del contrasto giurisprudenziale dianzi delineato, il Collegio della Quinta

Sezione, *ex* art. 618 cod. proc. pen., ha rimesso i ricorsi alle Sezioni Unite, ed il Primo Presidente, con decreto in data.24 giugno 2011, ne ha disposto la trattazione alla odierna pubblica udienza.

CONSIDERATO IN DIRITTO

1. La questione di diritto per la quale i ricorsi sono stati rirnessi alle Sezioni Unite è la seguente: *«se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita».*

2. Il quesito inerisce alla fattispecie criminosa, introdotta dalla legge 23 dicembre 1993, n. 547 e prevista dall'art. 615-ter cod. pen., che sanziona (primo comma) il fatto di *«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero ivi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo».*

Le condotte punite da tale norma, *a dolo generico,* consistono pertanto:

a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza: da intendersi come accesso alla conoscenza dei dati o informazioni contenuti nel sistema, effettuato sia da lontano (attività tipica *dell'hacker)* sia da vicino (da persona, cioè, che si trova a diretto contatto dell'elaboratore);

b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione: da intendersi come il persistere nella già avvenuta introduzione, inizialmente autorizzata o casuale, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema. Ipotesi tipica è quella in cui l'accesso di un soggetto sia autorizzato per il compimento di operazioni determinate e per il relativo tempo necessario (ad esempio, l'esecuzione di uno specifico lavoro ovvero l'installazione di un nuovo programma) ed il soggetto medesimo, compiuta l'operazione espressamente consentita, si intrattenga nel sistema per la presa di conoscenza, non autorizzata, dei dati.

3. La controversia interpretativa che ha portato alla rimessione dei ricorsi in oggetto alle Sezioni Unite si incentra sulla configurabilità del reato nel caso in cui un soggetto, legittimamente ammesso ad un sistema informatico o telematico, vi operi per conseguire finalità illecite.

Sul punto si rinviene effettivamente un contrasto nella giurisprudenza di questa Corte.

3.1 Un primo orientamento ritiene che il reato dl cui al primo comma dell'art. 615-ter cod. pen. possa essere integrato anche dalla condotta del soggetto che, pure essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la *password* di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, utilizzando sostanzialmente il sistema per finalità diverse da quelle consentite.

Tale orientamento si fonda sostanzialmente sulla considerazione che la norma in esame punisce non soltanto l'abusiva introduzione nel sistema (da escludersi nel caso di possesso del titolo di legittimazione) ma anche l'abusiva permanenza in esso contro la volontà di chi ha il diritto di escluderla: volontà contraria tacita in caso di perseguimento di una finalità illecita incompatibile con le ragioni per le quali l'autorizzazione all'accesso sia stata concessa.

L'opzione esegetica in oggetto è stata motivata anzitutto sulla base della ravvisata analogia con la fattispecie della violazione di domicilio, considerandosi che entrambi gli illeciti sono caratterizzati dalla manifestazione di una volontà contraria a quella, anche tacita, di chi ha diritto di ammettere ed escludere l'accesso e di consentire la permanenza (nei sistema informatico alla stessa stregua che nel domicilio).

Se il titolo di legittimazione all'accesso viene utilizzato dall'agente per finalità diverse da quelle consentite, dovrebbe ritenersi che la permanenza nel sistema informatico avvenga contro la volontà del titolare del diritto di esclusione. Pertanto 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; in tale ipotesi ciò che si punisce è l'uso dell'elaboratore avvenuto con modalità non consentite, più che l'accesso ad esso.

In questo senso ha argomentato, per la prima volta la Quinta Sezione, con la sentenza n. 12732 del 07/11/2000, Zara, concernente una vicenda in cui un soggetto, essendo

autorizzato solo all'accesso «per controllare la funzionalità del programma informatico», si era indebitamente avvalso di tale autorizzazione «per copiare i dati in quel programma inseriti», rilevando che «il delitto di violazione di domicilio è stato notoriamente il modello dì questa nuova fattispecie penale, tanto .da indurre molti a individuarvi, talora anche criticamente, la tutela di un *domicilio informatico».*
Analoghe considerazioni sono state svolte dalla Seconda Sezione, con la sentenza n. 30663 del 04/05/2006, Grimoldi, ed ulteriormente sviluppate dalla Quinta Sezione con la sentenza n. 37322 del 08/07/2008, Bassani, dove è stato posto in evidenza 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 ci manomissioni non autorizzate. Tra i beni e gli interessi tutelati non vi è alcun dubbio [...] che particolare rilievo assume la tutela dei 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 exdudendi alios* quale che sia il contenuta dei dati [...]. 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 c.d. *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'art. 14 Cost., e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 cod. pen.».
La sentenza n. 37322 del 2008 ha ribadito che «la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sé, perché non si tratta di un illecito caratterizzato dalla effrazione dei sistemi protettivi, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone.[...] L'accesso al sistema è consentito dal titolare per determinate finalità, cosicché se il titolo di legittimazione all'accesso viene dall'agente utilizzato per finalità diverse da quelle consentite non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione».
L'orientamento in oggetto ha trovato successivamente accoglimento in ulteriori pronunzie della Quinta Sezione:
La sentenza n. 18006 del 13/02/2009, Russo, ha applicato il principio ad una fattispecie relativa all'indebita acquisizione, con la complicità di appartenenti alla Polizia di Stato, di notizie riservate tratte dalla banca-dati del sistema telematico di informazione interforze del Ministero dell'Interno, per l'utilizzo in attività di investigazione privata di agenzie facenti capo agli stessi indagati o alle quali essi collaboravano.
La sentenza n. 2987 del 10/12/2009, dep. 2010, Matassich, ha ribadito l'orientamento in relazione alla copiatura, da parte di dipendenti, dei *files* presenti nella memoria del *computer* della azienda ove essi prestavano lavoro.
La sentenza n. 19463 del 16/02/2010, Jovanovic, ha ravvisato la configurabilità del reato di cui all'art. 615-ter cod. pen. per «il pubblico ufficiale che, pur avendo titolo e formale legittimazione per accedere ad un sistema informatico o telematico, vi si introduca su altrui istigazione criminosa nel contesto di un accordo di corruzione propria». In tal caso già l'accesso del pubblico ufficiale - che, in seno ad un reato plurisoggettivo finalizzato alla commissione di atti contrari ai doveri d'ufficio (art. 319 cod. pen.), diventi la *longa manus* del promotore del disegno delittuoso - è stato ritenuto in sé "abusivo" e integrativo della fattispecie incriminatrice di cui all'art. 615-ter cod. pen., in quanto «effettuato al di fuori dei compiti d'ufficio e preordinato all'adempimento dell'illecito accordo con il terzo, indipendentemente dalla permanenza nel sistema contro la volontà di chi ha il diritto di escluderlo».
Secondo tale pronuncia, «tanto sposta l'attenzione dal momento della permanenza nel

sistema contro la volontà di chi ha il diritto di escluderlo, a quello dell'accesso ed è lo stesso atto di accesso a qualificarsi come integrativo del reato, a prescindere dal prosieguo della condotta».
La sentenza n. 39620 del 22/09/2010, dep. 2010, Lesce, ha ritenuto integrato il delitto di accesso abusivo ad un sistema informatico o telematico dalla «condotta di colui che, in qualità di agente della Polstrada, addetto al terminale del centro operativo sezionale, effettui un'interrogazione al CED banca dati del Ministero dell'Interno, relativa ad una vettura, usando la sua *password* e l'artifizio delta richiesta di un organo di Polizia in realtà inesistente, necessaria per accedere a tale informazione» (per accedere alla banca dati del Ministero dell'Interno e necessario, infatti, che l'operatore utilizzi una *password* che lo abiliti alla richiesta e che indichi l'organo di Polizia Giudiziaria richiedente; laddove nella fattispecie concreta l'imputato aveva indicato un organo richiedente, che, invece, non aveva richiesto assolutamente nulla ed aveva altresì omesso di annotare la fittizia operazione sull'apposito registro della sala operativa, documento destinato a provare i fatti e le attività del servizio).
3.2 Un altro orientamento - del tutto difforme - esclude in ogni caso che il reato di cui all'art. 615-ter cod. pen. sia integrato dalla condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate.
A sostegno di tale interpretazione, sì osserva anzitutto che la sussistenza della volontà contraria dell'avente diritto, cui fa riferimento la norma incriminatrice, deve essere verificata esclusivamente con riguardo al risultato immediato della condotta posta in essere dall'agente con l'accesso al sistema informatico e con il mantenersi al suo interno, e non con riferimento a fatti successivi (l'uso illecito dei dati) che, anche se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente.
Un ulteriore argomento viene tratto dalla formula normativa "abusivamente si introduce", la quale, per la sua ambiguità, potrebbe dare luogo ad imprevedibili e pericolose dilatazioni della fattispecie penale se non fosse intesa nel senso di "accesso non autorizzato", secondo la più corretta espressione di cuialla c.d. "lista minima" della Raccomandazione R(89)9 del Comitato dei Ministri del Consiglio d'Europa, sulla criminalità informatica, approvata il 13 settembre 1989 ed attuata in Italia con la legge n. 547 del 1993, e, quindi, della locuzione "accesso senza diritto" *(access [...] without right)* impiegata nell'art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica *(cyber crime)* fatta a Budapest il 23 novembre 2001 e ratificata con la legge 18 marzo 2008, n. 48. Peraltro, come per ogni norma che rappresenta la trasposizione o l'attuazione di disposizioni sovranazionali, anche per l'art. 615-ter cod. pen. va privilegiata, tra più possibili letture, quella di senso più conforme a tali disposizioni.
Questo orientamento è stato illustrato dalla Quinta Sezione con la sentenza n. 2534 del 20/12/2007, dep. 2008, Migliazzo, ove si è affermato che «non integra il reato di accesso abusivo ad un sistema informatico (art. 615-ter cod. pen.) la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, si introducano nel sistema denominata S.D.I. (banca dati interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi ad una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo dì reato» (nella fattispecie è stata considerata altresì ininfluente la circostanza che detto uso fosse stato già previsto dall'agente all'atto dell'acquisizione e ne avesse costituito la motivazione esclusiva).
Secondo le argomentazioni svolte nella sentenza Migliazzo, «se dovesse ritenersi che, ai fini della consumazione del reato, basti l'intenzione, da parte del soggetto autorizzato all'accesso al sistema informatico ed alla conoscenza dei dati ivi contenuti, di fare poi un uso illecito di tali dati, ne deriverebbe l'aberrante conseguenza che il reato non sarebbe escluso neppure se poi quell'uso, di fatto, magari per un ripensamento da parte del medesimo soggetto agente, non vi fosse più stato».
L'interpretazione restrittiva del contenuto della norma è stata poi ulteriormente

sviluppata dalla Quinta Sezione con la sentenza n. 26797 del 29/05/2008, Scimia (ove è stato escluso che dovesse rispondere del reato in questione un funzionario di cancelleria il quale, legittimato in forza della sua qualifica ad accedere al sistema informatico dell'amministrazione giudiziaria, lo aveva fatto allo scopo di acquisire notizie riservate che aveva poi indebitamente rivelate a terzi con i quali era in previo accordo; condotta, questa, ritenuta integratrice del solo reato di rivelazione di segreto d'ufficio, previsto dall'art. 326 cod. pen.).
In tale decisione è stato escluso che l'imputato avesse effettuato un accesso non consentito o si fosse indebitamente trattenuto, oltre modi o tempi permessi, nei registri informatizzati dell'amministrazione della giustizia, poiché l'interrogazione era stata effettuata con la utilizzazione della chiave logica (o *password)* legittimamente in suo possesso. E' stato altresì evidenziato che non solo non esiste norma o disposizione interna organizzativa che inibisca al cancelliere addetto alla singola sezione di consultare i dati del registro generale e le assegnazioni ai diversi uffici (giacché nessuna limitazione di tal genere è prevista per la lettura dei dati ad opera degli utilizzatori del sistema), ma una inibizione siffatta sarebbe contraria ad ogni buona regola organizzativa, attese le necessità di consultazione di un ufficio giudiziario.
Alle stesse conclusioni è pervenuta pure la Sesta Sezione, con la sentenza n. 39290 del 08/10/2008, Peparaio, secondo cui «nella fattispecie di cui all'art. 615-ter cod. pen. sono delineate due diverse condotte integratici del delitto; la prima consiste nel fatto di "chi abusivamente si introduce in un sistema informatico o telematico protetto da misura di sicurezza", la seconda nel fatto di chi "vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo". La qualificazione di 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 (chiavi fisiche o elettroniche, *password, etc.)* apprestate dal titolare dello *ius excludendi,* al fine di selezionare gli ammessi al sistema ed impedire accessi indiscriminati. Il reato è integrato dall'accesso non autorizzato nel sistema informatico, ciò che di per sé mette a rischio la riservatezza del domicilio informatico, indipendentemente dallo scopo che si propone l'autore dell'accesso abusivo. La finalità dell'accesso, se illecita, integrerà eventualmente un diverso titolo di reato. Non può, pertanto, condividersi l'interpretazione della norma che individua l'abusività della condotta nel fatto del pubblico ufficiale o dell'incaricato di pubblico servizio che, abilitato ad accedere al sistema informatico, usi tale facoltà per finalità estranee all'ufficio e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Tale lettura della norma finisce con l'intrecciare le due condotte descritte dall'art. 615-ter cod. pen., che sono differenti e alternative, disgiuntamente considerate dal legislatore. Sarebbe stata pleonastica la descrizione della seconda condotta se la prima fosse integrata anche da chi usa la legittimazione all'accesso per fini diversi da quelli a cui è stato legittimato dal titolare del sistema».
L'indirizzo in esame è stato seguito poi dalla Quinta Sezione con la sentenza n. 40078 del 25/06/2009, Genchi.
4. A fronte del contrastante quadro interpretativo dianzi delineato, queste Sezioni Unite ritengono che la questione di diritto controversa non debba essere riguardata sotto il profilo delle *finalità* perseguite da colui che accede o si mantiene nel sistema, in quanto la volontà del titolare del diritto di escluderlo si connette soltanto al *dato oggettivo* della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi.
Rilevante deve ritenersi, perciò, il *profilo oggettivo* dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro) sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito.
In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che

risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta.
Il dissenso tacito del *dominus loci* non viene desunto dalla finalità (quale che sia) che anima la condotta dell'agente, bensì dall'oggettiva violazione delle disposizioni dei titolare in ordine all'uso del sistema. Irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuoti atti volitivi e pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato (rientrando, ad esempio, nelle previsioni di cui agli artt.. 326, 618, 621 e 622 cod. pen.).
Ne deriva che, nei casi in cui l'agente compia sul sistema un'operazione pienamente assentita dall'autorizzazione ricevuta, ed agisca nei limiti di questa, il reato di cui all'art. 615-ter cod. pen. non è configurabile, a prescindere dallo scopo eventualmente perseguito; sicché qualora l'attività autorizzata consista anche nella acquisizione di dati informatici, e l'operatore la esegua nei limiti e nelle forme consentiti dal titolare dello *ius excludendi,* il delitto in esame non può essere individuato anche se degli stessi dati egli si dovesse poi servire per finalità illecite.
Il giudizio circa l'esistenza del dissenso del *dominus loci* deve assumere come parametro la sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della condotta, soggettivamente intesa.
Vengono in rilievo, al riguardo, quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, da prendere necessariamente in considerazione, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati.
5 Va affermato, in conclusione, il principio di diritto secondo il quale *«integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art.* 615-ter *cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Nonhanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema».*
6. Alla stregua di tale principio deve essere esaminata, dunque, la vicenda oggetto del processo, caratterizzata - secondo gli accertamenti di fatto e le acquisizioni dibattimentali - dalla circostanza che il maresciallo S. era stato autorizzato ad accedere al sistema informatico interforze ed a consultare lo stesso soltanto per ragioni «di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione dei reati», con espresso divieto dì stampare il risultato delle interrogazioni «se non nei casi di effettiva necessità e comunque previa autorizzazione da parte del comandante diretto».
Trattasi di prescrizioni disciplinanti l'accesso ed il mantenimento all'interno del sistema che, in quanto non osservate dall'imputato, hanno reso abusiva l'attività di consultazione esercitata in concreto, prescindendosi dai successivo uso indebito dei dati acquisiti e dalla predeterminazione di unafinalità siffatta.
La condotta è stata posta in essere con la consapevolezza della contrarietà alte disposizioni ricevute e, quindi, del carattere *invito domino* dell'accesso e della permanenza fisica nel sistema, e ciò integra ad evidenza il dolo generico richiesto dalla norma, che non prevede alcuna finalità speciale né io scopo di trarre profitto, per sé o per altri, ovvero di cagionare ad altri un danno ingiusto.
Le doglianze riferite, nel ricorso del S., alla configurabilità del delitto di cui all'art. 615-ter cod. pen. devono essere conseguentemente rigettate, perché infondate.
7. Infondate sono altresì le questioni svolte nei tre ricorsi con riferimento alla ravvisabilità, rispetto alla fattispecie concreta, del reato di rivelazione ed utilizzazione di segreti di ufficio: reato del quale viene prospettata l'esclusione sotto i profili sia della mancanza di un pericolo effettivo per gli interessi protetti dalla norma incriminatrice, sia della mancanza di prova del dolo.
La giurisprudenza di questa Corte, che il Collegio condivide e ribadisce, configura il

delitto di cui all'art. 326 cod. pen. quale reato di *pericolo effettivo* (e non meramente presunto) per gli interessi tutelati, nel senso che la rivelazione del segreto è punibile, non già in sé e per sé, ma in quanto suscettibile di produrre nocumento, alla pubblica amministrazione o ad un terzo, a mezzo della notizia da tenere segreta. Ne consegue che il reato non sussiste, oltre che nella generale ipotesi della notizia divenuta di dominio pubblico, qualora notizie d'ufficio ancora segrete siano rivelate a persone autorizzate a riceverle (e cioè che debbono necessariamente esserne informate per la realizzazione dei fini istituzionali connessi al segreto di cui si tratta) ovvero a soggetti che, ancorché estranei ai meccanismi istituzionali pubblici, le abbiano già conosciute, fermo restando per tali ultime persone il limite della non conoscibilità dell'evoluzione della notizia oltre i termini dell'apporto da esse fornito (vedi Sez. 6, n. 9306 del 06/06/1994, Bandiera; Sez. 5, n. 30070 del 20/03/2009, C.).
Le ipotesi di non punibilità del reato di cui all'art. 326 cod. pen. per inoffensività del fatto risultano comunque limitate a casi assai circoscritti, essendo stato evidenziato dalla giurisprudenza di legittimità che:
- il reato di rivelazione di segreti di ufficio si configura anche quando il fatto coperto dal segreto sia già conosciuto in un ambito limitato di persone e la condotta dell'agente abbia avuto l'effetto di diffonderlo in un ambito più vasto (Sez. 6: n. 929 del 05/12/1997, dep. 1998, Colandrea; Sez. 6, n. 35647 del 17/05/2004, Vietti);
- gli interessi tutelati dalla fattispecie incriminatrice in oggetto si intendono lesi allorché la divulgazione della notizia sia anche soltanto suscettibile di arrecare pregiudizio alla pubblica amministrazione o ad un terzo (Sez. 5, n. 46174 del 05/10/2004, Esposito; Sez. 1, n. 1265 del 29/11/2006, dep. 2007, Bria; Sez. 6, n. 5141 del 18/12/2007, dep. 2008, Cincavalli);
- quando è la legge a prevedere l'obbligo del segreto in relazione ad un determinato atto o in relazione ad un determinato fatto, il reato sussiste senza che possa sorgere questione circa l'esistenza o la potenzialità del pregiudizio richiesto, in quanto la fonte normativa ha già effettuato la valutazione circa l'esistenza del pericolo, ritenendola conseguente alla violazione dell'obbligo del segreto (Sez. 6, *n.* 42726 dell'11/10/2005, De Carolis);
- integra il concorso nel delitto di rivelazione di segreti d'ufficio la divulgazione da parte dell'*extraneus* del contenuto di informative dl reato redatte da un ufficiale di polizia giudiziaria, realizzandosi in tal modo una condotta ulteriore rispetto a quella dell'originario propalatore (Sez. 6, n. 42109 del 14/10/2009, Pezzuto).
Ora, nella fattispecie in esame non risulta dimostrato che il C. e lo stesso M. avessero conoscenza del contenuto specifico ed integrale delle informative redatte da ufficiali della polizia giudiziaria in relazione ai comportamenti posti in essere da quest'ultimo considerati illeciti; e, in relazione ai fatti divulgati, poiché l'obbligo del segreto è precipuamente previsto dalla legge, non può sorgere questione circa l'esistenza o la potenzialità di produrre nocumento, a mezzo della notizia da tenere segreta, alla pubblica amministrazione o ad un terzo, proprio perché la fonte normativa ha già effettuato la valutazione circa l'esistenza di un pericolo siffatto, ritenendola conseguente già alla mera violazione dell'obbligo del segreto.
Quanto al profilo del dolo, va evidenziato che il reato di cui all'art. 326 cod. pen. è punibile a titolo di dolo generico, consistente nella volontà consapevole della rivelazione e nella coscienza che la notizia costituisce un segreto di ufficio, essendo, perciò, irrilevante il movente ovvero la finalità della condotta e senza che possa aver alcun valore esimente l'eventuale errore sui limiti dei propri e degli altrui poteri e doveri in ordine a dette notizie (vedi Sez. 6, n. 2183 del 13/01/1999, Curia; Sez. 6, n. 9331 dell'11/02/2002, Fortunato).
La sussistenza di tale volontà consapevole, nella vicenda in esame, risulta adeguatamente illustrata dai giudici del merito.
Segue il rigetto integrale dei gravami proposti da G. C. e A. T.
8. Priva di fondamento deve ritenersi pure l'eccezione svolta nel ricorso dell'imputato S., con cui si prospetta l'erronea applicazione dell'art. 599, comma 2, cod. proc. pen., (dalla quale sì fa discendere la conseguente nullità del giudizio e della sentenza impugnata), a cagione della pretesa illegittimità del diniego del differimento dell'udienza camerale davanti alla Corte di appello, chiesto dal ricorrente per infermità documentata da

certificato medico.
L'art. 599, comma 2, cod. proc. pen. dispone che, per il giudizio camerate d'appello avverso la sentenza pronunciata con il rito abbreviato, il legittimo impedimento dell'imputato comporta il rinvio dell'udienza soltanto allorché l'imputato stesso abbia manifestato in qualsiasi modo la volontà di comparire (cfr. Sez. U, n. 35399 del 24/6/2010, F.).
La giurisprudenza di questa Corte è divisa in ordine alla individuazione delle modalità attraverso cui tale volontà può essere legittimamente manifestata.
A fronte, però, di un indirizzo interpretativo secondo il quale «nel giudizio di appello contro la sentenza pronunciata all'esito del giudizio abbreviato non trova applicazione l'istituto della contumacia dell'imputato, sicché il legittimo impedimento dello stesso impone il rinvio dell'udienza solo se egli abbia direttamente e tempestivamente manifestato la volontà di comparire, non essendo sufficiente a tale fine la mera istanza di rinvio avanzata dal difensore allegante l'impedimento» (così da ultimo, Sez. 2, n. 8040 del 09/02/2010, Fiorito), il Collegio ritiene maggiormente conforme al compiuto esercizio dei diritti della difesa il diverso orientamento secondo il quale «la richiesta di partecipazione da parte dell'imputato di cui all'art. 599, comma 2, cod. proc. pen. può essere tratta anche da *facta concludentia* (quale la produzione, da parte del difensore, di una certificazione medica attestante l'impedimento a comparire dell'imputato con espressa istanza di rinvio) da cui possa desumersi la inequivoca manifestazione della volontà dell'imputato medesimo di comparire all'udienza camerale» (vedi Sez. 6, n. 1320 del 14/10/1996, Surace; Sez. 6, n. 43201 dell'11/10/2004, Viti; Sez. 6, n. 2811 del 18/12/2006, dep.. 2007, Ramelli).
Quanto ai poteri valutativi del giudice rispetto alle ragioni di salute documentate in un certificato medico prodotto a sostegno della richiesta di rinvio dell'udienza, le Sezioni Unite - con la sentenza n. 36635 del 27/09/2005, Gagliardi - si sono pronunciate nel senso che «in tema di impedimento a comparire dell'imputato, il giudice, nel disattendere un certificato' medico ai fini della dichiarazione di contumacia, deve attenersi alla natura dell'infermità e valutarne il carattere impeditivo, potendo pervenire ad un giudizio negativo circa l'assoluta impassibilità a comparire solo disattendendo, con adeguata valutazione del referto, la rilevanza della patologia da cui si afferma colpito l'imputato».
Con riferimento a tale necessaria valutazione, comunque, va ribadito che:
- «il legittimo impedimento a comparire dell'imputato, oltre che grave e assoluto, deve presentare il carattere dell'attualità e cioè deve sussistere in relazione all'udienza per la quale egli è stato citato, in quanto l'impossibilità a presenziare alla stessa deve risultare dagli elementi addotti, come non altrimenti superabile» (così Sez. 5, n. 3392 del 14/12/2004, dep. 2005, Curaba; Sez. 4, n. 5901 del 15/03/1995, Maciocchi);
- «il giudice di merito non ha alcun obbligo di disporre accertamenti fiscali per accertare l'impedimento dell'imputato a comparire al dibattimento, al fine di completare la insufficiente documentazione prodotta, purché dia ragione del suo convincimento di non assolutezza dell'impedimento con motivazione logica e corretta» (Sez. 1, n. 6241 del 02/04/1990, Sforza).
Dopo la citata pronunzia delle Sezioni Unite, inoltre, è stato ribadita la legittimità del provvedimento di diniego della richiesta di rinvio per impedimento dell'imputato a comparire, in ipotesi di produzione di un certificato medico che si limiti:
- ad attestare l'infermità (nella specie, faringo-tracheite) con esiti febbrili e la prognosi, senza indicare il grado della febbre, essenziale alla valutazione della fondatezza, serietà e gravità dell'impedimento (Sez. 6, n. 20811 del 12/05/2010, dep. 3/6/2010, S.);
- ad attestare l'infermità di per sé non invalidante (nella specie, colica renale) e la prognosi, senza nulla affermare in ordine alla determinazione dell'impossibilità fisica assoluta di comparire (Sez. 6, n. 24398 del 26/02/2008, De Macceis).
Ora, nella fattispecie in esame, all'udienza del 19 maggio 2009, risulta presentato certificato medico riferito al S., redatto il precedente 15 maggio ed attestante che l'imputato era affetto da "cistite emorragica febbrile" e necessitava "di giorni sei di riposo e cure".
Alla stregua della consolidata giurisprudenza di questa Corte (di cui si è dato conto dianzi), pertanto, deve considerarsi assolutamente corretta la decisione del giudice di

merito che ha rigettato l'istanza di rinvio sui rilievi che: a) il certificato era stato redatto quattro giorni prima dell'udienza; *b)* in esso non era indicato il grado febbrile; c) nulla veniva affermato in ordine alla determinazione dell'impossibilità fisica assoluta di comparire, attestandosi esclusivamente la necessità "di riposo e cure".

9. L'unico motivo di ricorso che deve ritenersi fondato è quello riferito al trattamento sanzionatorio nell'atto di gravame proposto nell'interesse del S., ove (sia pure con diversa doglianza) si prospetta che le condotte indicate nel secondo comma, n. 1, dell'art. 615-ter cod. pen. non integrano fattispecie delittuose distinte ed autonome rispetto a quelle descritte nel primo comma, costituendo invece ipotesi aggravate finalizzate ad innalzare la sanzione da applicare a quei soggetti che in ragione della loro funzione - e purché non legittimati *ab initio* - sono facilitati ad attingere informazioni sensibili.

9.1. Va rilevato, sul punto, che la sezione 5, con la sentenza n. 1727 del 30/09/2008, dep. 2009, Romano, ha differenziato nettamente la portata applicativa delle fattispecie rispettivamente contemplate dal comma primo e dal comma secondo, n. 1, dell'art. 615-ter cod. pen., affermando che «l'accesso abusivo *ad* un sistema informatico (art. 615-ter, comma primo, cod. pen.) e l'accesso commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione del doveri o con abuso della qualità di operatore del sistema (art. *615-ter,* comma secondo, n. 1) configurano due distinte ipotesi di reato, l'applicabilità di una delle quali esclude l'altra secondo il principio di specialità; concernendo il comma primo l'accesso abusivo ovvero l'intrusione da parte di colui *che* non sia in alcun modo abilitato, mentre il comma secondo - non costituisce una mera aggravante - ma concerne il caso in cui soggetti abilitati all'accesso abusino di detta abilitazione».

Tale impostazione risulta ribadita, sempre dalla Quinta Sezione, nella recente sentenza n. 24583 del 18/01/2011, Tosinvest, secondo la quale il secondo comma, n. 1, dell'art. 615-ter cod. peri. non costituisce un'aggravante del fatto descritto nel primo comma, ma un'ipotesi diversa di reato, perché la disposizione si riferisce evidentemente a soggetti ordinariamente abilitati ad entrare nel sistema, il cui accesso sarebbe, pertanto, di regola legittimo, ma diviene penalmente rilevante quando i predetti abbiano fatto abuso di tale loro abilitazione.

9.2 Le pronunzie anzidette non sono condivise da questo Collegio sulla base delle seguenti considerazioni:

a) "circostanze del reato" sono quegli elementi che, non richiesti per l'esistenza del reato stesso, laddove sussistono incidono sulla sua maggiore o minore gravità, così comportando modifiche quantitative o qualitative all'entità della pena: trattasi di elementi che si pongono in rapporto di *species a genus* (e non come fatti giuridici modificativi) con i corrispondenti elementi della fattispecie semplice in modo da costituirne, come evidenziato da autorevole dottrina, «una specificazione, un particolare modo d'essere, *una* variante di intensità di corrispondenti elementi generali»;

b) il problema, in materia, è quello di individuare un criterio per identificare le disposizioni normative che prevedono appunto "circostanze" in senso tecnico e quelle che, invece, prevedono elementi costitutivi della fattispecie, e queste Sezioni Unte - con la sentenza n. 26351 del 10/07/2002, Fedi (che ha individuato nel reato previsto dall'art. 640-bis cod. pen. semplicemente una figura aggravata del delitto di truffa) - hanno ritenuto che l'unico criterio idoneo a distinguere le norme che prevedono circostanze da quelle che prevedono elementi costitutivi della fattispecie è il criterio strutturale della descrizione del precetto penale;

c) nei casi previsti dall'art. 615-ter, comma secondo, n. 1, cod. pen. non vi è immutazione degli elementi essenziali delle condotte illecite descritte dal primo comma, in quanto il riferimento è pur sempre a quei fatti-reato, i quali vengono soltanto integrati da qualità peculiari dei soggetti attivi delle condotte, con specificazioni meramente dipendenti dalle fattispecie di base.

La configurata aggravante si riferisce a soggetti che possono legittimamente contattare il sistema informatico (secondo le prescrizioni e le limitazioni imposte dal *dominus loci),* stante il collegamento funzionale con lo stesso per ragioni inerenti i propri compiti professionali, ma che accedono ad esso e vi si trattengono in violazione dei doveri inerenti allo loro funzione nonché dei limiti dell'uso legittimo loro riconosciuti.

Il più rigoroso trattamento sanzionatorio e la procedibilità di ufficio trovano evidente giustificazione nel momento abusivo della qualità soggettiva, che rende più agevole per l'agente la realizzazione della condotta tipica.

9.3 Deve affermarsi pertanto l'ulteriore principio di diritto (conforme peraltro al concorde orientamento della dottrina) secondo il quale *«l'ipotesi dell'abuso delle qualità specificate dall'art.* 615-ter, *comma secondo, n. i, cod. pen., costituisce una circostanza aggravante delle condotte illecite descritte al primo comma e non un'ipotesi autonoma di reato».*

9.4 Nella vicenda in esame la responsabilità del S. è stata ravvisata in ordine al delitto

di cui all'art. 615-ter, comma secondo, n. 1, e comma terzo, cod. pen., sicché la Corte di merito avrebbe dovuto operare il giudizio di bilanciamento delle riconosciute attenuanti generiche con ledue circostanze aggravanti *(ex* art. 69cod. pen.).
Non può dubitarsi infatti - alla stregua dei principi fissati da queste Sezioni Unite con la già ricordata sentenza n. 26351 del 2002 - della natura meramente aggravatrice anche dell'ipotesi prevista dal terzo comma (non costituente oggetto del ricorso), che, senza modificare gli elementi essenziali del fatto-reato, introduce una sanzione più rigorosa per la particolare rilevanza pubblica del sistema riconosciuta dal legislatore in connessione ai dati ed alle informazioni peculiari in esso contenute.
Ne consegue che la sentenza impugnata deve essere annullata, nei confronti di G. S., limitatamente al trattamento sanzionatorio, con rinvio, per una nuova effettuazione dei giudizio di comparazione tra le circostanze e per la determinazione della pena, ad altra sezione della Corte di appello di Roma.
10. Al rigetto integrale dei ricorsi del C. e della T. segue la condanna degli stessi al pagamento delle spese processuali.
Tutti i ricorrenti, infine, devono essere condannati, con vincolo solidale, alla rifusione delle spese di parte civile del presente grado di giudizio, che si ritiene di liquidare, in relazione all'attività processuale svolta, in euro 3.000,00 oltre accessori.

P.Q.M.

Annulla la sentenza impugnata, nei confronti di S. G. limitatamente al trattamento sanzionatorio, e rinvia ad altra sezione della Corte di appello di Roma.
Rigetta il ricorso dei S. nel resto.
Rigetta i ricorsi di C. G. e T. A., che condanna al pagamento delle spese processuali.
Condanna in solido i tre ricorrenti alla rifusione delle spese di parte civile del presente grado, che liquida in euro 3.000,00 oltre accessori.
Così deciso il 27 ottobre 2011.
Il componente estensore Il Presidente
Aldo Fiale Ernesto Lupo