Risponde del delitto di accesso abusivo ad un sistema informatico ex art. 615 ter c.p. il pubblico ufficiale che, pur accedendo mediante le proprie credenziali, si trattenga all'interno del sistema per finalità estranee all'espletamento del proprio ufficio.

CORTE DI CASSAZIONE, SEZIONI UNITE , SENTENZA 8 settembre 2017, n.41210 - Pres. Canzio – est. Savani

Ritenuto in fatto

1. S.A.G. è stata tratta a giudizio davanti al Tribunale di Busto Arsizio per rispondere del reato p. e p. dagli artt. 81 cpv., 615-ter, primo comma e secondo comma, n. 1, cod. pen., perché, con più atti esecutivi di un medesimo disegno criminoso, essendo autorizzata nella propria qualità di cancelliere in servizio presso la Procura della Repubblica di Busto Arsizio ad accedere al registro delle notizie di reato Re.Ge., vi si manteneva in violazione dei limiti e delle condizioni risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, in particolare accedendo alle informazioni inerenti il procedimento penale a carico di C.C. (assegnato a sostituto procuratore diverso da quello presso cui l'indagata prestava servizio e relativo ad un suo conoscente), nelle seguenti date ed orari: alle ore 13.37 e alle ore 16.43 del (omissis) . Con l'aggravante dell'essere stato commesso il fatto da un pubblico ufficiale con abuso dei poteri e violazione dei doveri inerenti la funzione o il servizio.

2. La S. da quel reato, così come anche dal contestato delitto di rivelazione di segreti di ufficio, per la comunicazione al C. dei dati acquisiti dal sistema, era stata assolta dal Tribunale, sul rilievo che essa era titolare delle credenziali per accedere alle informazioni contenute nell'intero sistema, non essendo ravvisabile una contraria volontà da parte del gestore del sistema, in quanto, su disposizioni organizzative interne del Procuratore aggiunto della Repubblica, i pubblici ministeri ed i soggetti autorizzati come lei avevano accesso a tutti i procedimenti iscritti al Re.Ge., non essendo quindi emerse violazioni dei limiti risultanti dal complesso delle prescrizioni impartite all'agente, né che fossero state realizzate "operazioni di natura ontologicamente diversa da quelle cui l'operatore era incaricato ed in relazione alle quali l'accesso era consentito".

3. La Corte di appello di Milano, in accoglimento dell'impugnazione del Pubblico Ministero, ha riformato la sentenza del Tribunale e dichiarato l'imputata colpevole del reato di accesso abusivo aggravato al sistema Re.Ge., condannandola alla pena ritenuta di giustizia.

Il giudice d'appello, premesso che l'ingresso e l'utilizzazione del sistema informatico Re.Ge. potrebbe avvenire legittimamente soltanto in presenza di un interesse pubblico che giustifichi accesso e permanenza dell'operatore, ha ritenuto che il fatto che l'imputata avesse visionato gli atti del procedimento penale iscritto a carico del C. , senza alcuna necessità di ufficio che lo potesse giustificare, integrava la fattispecie incriminatrice contestata in quanto riconducibile al concetto di operazione di accesso abusivo di natura

"ontologicamente diversa" da quelle autorizzate.

4. Ha proposto ricorso per cassazione l'imputata, deducendo violazione di legge e vizio di motivazione, sostenendo che non sarebbe configurabile la condotta tipica prevista dalla norma citata, atteso che essa aveva legittimo accesso al sistema informatico Re.Ge. nella sua totalità. Illogicamente, e con violazione della norma, quale interpretata nella sentenza Sez. U, n. 4694 del 27/10/2011, dep. 2012, Casani, la Corte di appello avrebbe considerato irrilevante l'autorizzazione di accesso indiscriminato al Re.Ge. concessa dal titolare del sistema a tutti i soggetti dotati di password, mentre avrebbe ritenuto rilevanti le "finalità ulteriori dell'accesso e del mantenimento nel sistema" che avrebbero determinato l'imputata all'azione.

5. La Quinta Sezione ha ritenuto necessaria una rimeditazione della sentenza delle Sezioni Unite Casani, che aveva risolto un contrasto di giurisprudenza ritenendo che non integrasse il reato la condotta di chi, avendo titolo per accedere al sistema, se ne fosse avvalso per finalità estranee a quelle di ufficio.

Per la Sezione rimettente, la giurisprudenza formatasi in epoca successiva alla citata sentenza aveva manifestato l'esigenza di ulteriori precisazioni e specificazioni, in funzione estensiva, della portata del principio di diritto espresso dalle Sezioni Unite, tanto da ritenere idonea ad integrare la tipicità della fattispecie incriminatrice la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si traduca in un abuso o sviamento dei poteri conferitigli.

6. Il Primo Presidente, con decreto in data 21 marzo 2017, ha assegnato il ricorso alle Sezioni Unite, disponendone la trattazione alla odierna pubblica udienza.

Considerato in diritto

1. La questione di diritto sottoposta alle Sezioni unite è la seguente:

"Se il delitto previsto dall'art. 615-ter, secondo comma, n. 1, cod. pen., sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative".

2. L'art. 615-ter cod. pen. sanziona, al primo comma, il comportamento di chiunque "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo". Il secondo comma prevede: "La pena è della reclusione da uno a cinque anni: - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema".

L'accesso, quindi, è abusivo qualora avvenga mediante superamento e violazione delle chiavi fisiche ed informatiche di accesso o delle altre esplicite disposizioni su accesso e mantenimento date dal titolare del sistema.

3. Con la sentenza Casani le Sezioni Unite avevano affrontato la questione se integrasse la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema da parte di soggetto abilitato all'accesso, perché dotato di password, ma attuata per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli era stata attribuita.

Le Sezioni Unite hanno ritenuto che la questione di diritto controversa non dovesse 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 dell'agente in esso, dovendosi verificare la contraria volontà del titolare del sistema solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi. Avevano ritenuto, quindi, che rilevante dovesse considerarsi il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto non autorizzato ad accedervi ed a permanervi, sia quando violasse i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro), sia quando ponesse in essere operazioni di natura "ontologicamente diversa" da quelle di cui sarebbe stato incaricato ed in relazione alle quali l'accesso era a lui consentito, con ciò venendo meno il titolo legittimante l'accesso e la permanenza nel sistema.

4. La Sezione rimettente ha dato atto dello svilupparsi nella giurisprudenza successiva alla sentenza Casani di diverse posizioni, dettate dalla ritenuta necessità di precisazioni e specificazioni, in funzione eminentemente estensiva, della portata del principio di diritto espresso dalla citata sentenza, tanto da considerare idonea ad integrare la tipicità della fattispecie incriminatrice la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si traduca in un abuso o sviamento dei poteri conferitigli.

È stato, in particolare, evidenziato il contrasto manifestatosi con le sentenze, entrambe della Quinta Sezione, n. 22024 del 24/04/2013, Carnevale, Rv. 255387, e n. 44390 del 20/06/2014, Mecca, Rv. 260763, che, seppure fondate sulla espressa adesione all'identica premessa costituita dal decisum delle Sezioni Unite Casani, avevano fornito risposte antitetiche circa la possibilità di ravvisare l'abusività dell'accesso nella violazione dei principi che presiedono allo svolgimento dell'attività amministrativa, quali sinteticamente enunciate dall'art. 1 legge 7 agosto 1990, n. 241.

Secondo la prima decisione, nel caso in cui l'agente sia un pubblico dipendente "non può non trovare applicazione il principio di cui alla L. 7 agosto 1990 n. 241, art. 1, in base al quale l'attività amministrativa persegue fini determinati dalla legge ed è retta da criteri di economicità, efficacia, imparzialità, pubblicità, trasparenza, secondo le modalità previste dalla presente legge e dalle disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario". Di qui deriverebbe la "ontologica incompatibilità" di un utilizzo del sistema informatico senza il rispetto di tali principi, in quanto "fuoriuscente dalla ratio del conferimento del relativo potere".

Con la seconda delle citate decisioni era stata, all'opposto, esclusa la possibilità di identificare il carattere di abusività della condotta di accesso al sistema, o di mantenimento al suo interno, nella violazione delle predette regole di imparzialità e trasparenza enunciate dall'art. 1 legge n. 241 del 1990, se non a prezzo di frustrare la ratio della stessa norma incriminatrice come interpretata dalle Sezioni Unite, dilatando inammissibilmente la nozione di "accesso abusivo" oltre i limiti imposti dalla necessità di

tutelare i diritti del titolare del sistema.

Viene, di conseguenza, sottoposta ora alle Sezioni Unite la valutazione del non infrequente caso del soggetto, in specie pubblico ufficiale o equiparato, che, abilitato e senza precisazione di limiti espressi alle possibilità di accesso e trattenimento nel sistema pubblico, acquisisca da questo notizie e dati, in violazione dei doveri insiti nello statuto del pubblico dipendente, nel complesso degli obblighi e dei doveri di lealtà a lui incombenti.

5. Ritiene il Collegio che lo spunto fornito dalla vicenda processuale debba indurre a puntualizzare alcuni dei passaggi della precedente decisione delle Sezioni Unite Casani.

La vicenda oggetto del procedimento in corso contempla un accesso con credenziali al sistema Re.Ge., nonché specifiche letture di dati relativi a procedimento in carico a un pubblico ministero diverso da quello presso cui l'agente prestava servizio: accesso che, secondo le prospettazioni del ricorso, non sarebbe stato abusivo in virtù delle diposizioni organizzative interne del Procuratore aggiunto della Repubblica, dettate dall'esigenza di buona amministrazione di rendere disponibili i dati predetti per tutte le situazioni nelle quali i diretti titolari non potessero per un qualsiasi motivo accedervi.

La particolarità del caso e la precisa indicazione del quesito sviluppato dalla Sezione rimettente, centrato sulle condizioni per il ricorrere o meno dell'ipotesi aggravata prevista dall'art. 615-ter, secondo comma, n. 1, cod. pen., inducono il Collegio a concentrare il proprio esame sulla specifica previsione che descrive la condotta criminosa in quanto posta in essere dal pubblico ufficiale o da un incaricato di pubblico servizio.

6. In sintonia con le conclusioni della sentenza Casani, il Collegio rileva che quella prevista dal secondo comma, n. 1, della norma incriminatrice è qualificabile come circostanza aggravante esclusivamente soggettiva, nel senso che descrive la condotta punibile in quanto posta in essere da determinati soggetti. Il pubblico ufficiale, l'incaricato di pubblico servizio, l'investigatore privato e l'operatore del sistema possono rispondere del reato solo in forza della previsione del secondo comma Per tali soggetti il reato è sempre aggravato, proprio perché la circostanza è inscindibilmente collegata a quella qualità soggettiva ed in tutti i casi la configurata aggravante comporta un abuso, che ben può connotarsi delle caratteristiche dell'esecuzione di "operazioni ontologicamente estranee" rispetto a quelle consentite.

Invero la norma si riferisce a soggetti che accedono al sistema e vi si trattengono abusando della propria qualità soggettiva, che rende più agevole la realizzazione della condotta tipica, oppure che connota l'accesso in sé quale comportamento di speciale gravità.

Così, nel caso dell'investigatore privato, la cui attività professionale di indagine comporta limitazioni, essendo soggetta alla regolamentazione dell'art. 134 del TULPS ed al possesso della licenza prefettizia, che consente di eseguire investigazioni o ricerche o di raccogliere informazioni per conto di privati, con divieto di operazioni che importano una menomazione della libertà individuale, esercitando quindi un'attività sottoposta a controllo pubblico preventivo e successivo circa il rispetto delle attività di indagine che, secondo le relative norme, devono essere preventivamente pubblicizzate dai responsabili.

Ugualmente, abuso di speciale rilievo è quello dell'operatore di sistema che, abilitato

all’accesso al sistema proprio per la natura di manutenzione ed aggiornamento del sistema a lui affidato, oltrepassi i limiti connaturali allo svolgimento di quegli specifici compiti.

Altro abuso qualificato, per il quale si giustifica il più rigoroso trattamento sanzionatorio e la procedibilità di ufficio, è quello commesso dal pubblico ufficiale e dall’incaricato di pubblico servizio che, dotato di credenziali di accesso al sistema in uso presso l’ufficio di appartenenza, vi acceda o vi si trattenga in violazione dei doveri o con abuso dei poteri inerenti alla funzione o al servizio.

7. Nella giurisprudenza della Corte ripetuti sono gli esempi di violazione da parte di pubblico ufficiale o incaricato di pubblico servizio delle disposizioni del titolare del sistema concernenti le modalità di accesso, o più frequentemente di trattenimento e di utilizzo del sistema. Negli specifici casi viene in evidenza l’abuso del pubblico ufficiale in termini di violazione del dovere di rispetto delle norme che espressamente ne disciplinano l’azione, quali poste dai titolari del sistema.

Ad avviso del Collegio non esce dall’area di applicazione della norma la situazione nella quale l’accesso o il mantenimento nel sistema informatico dell’ufficio a cui è addetto il pubblico ufficiale o l’incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell’agente ed in assenza di ulteriori espressi divieti in ordine all’accesso ai dati, si connoti, tuttavia, dall’abuso delle proprie funzioni da parte dell’agente, rappresenti cioè uno sviamento di potere, un uso del potere in violazione dei doveri di fedeltà che ne devono indirizzare l’azione nell’assolvimento degli specifici compiti di natura pubblicistica a lui demandati.

Si è autorevolmente chiarito da parte della dottrina che "sotto lo schema dell’eccesso di potere si raggruppano tutte le violazioni di quei limiti interni alla discrezionalità amministrativa, che, pur non essendo consacrati in norme positive, sono inerenti alla natura stessa del potere esercitato".

Lo sviamento di potere è una delle tipiche manifestazioni di un tale vizio dell’azione amministrativa e ricorre quando l’atto non persegue un interesse pubblico, ma un interesse diverso (di un privato, del funzionario responsabile, ecc.). Si ha quindi "sviamento di potere" quando nella sua attività concreta il pubblico funzionario persegue una finalità diversa da quella che gli assegna in astratto la legge sul procedimento amministrativo (art. 1, legge n. 241 del 1990).

In tal senso il Collegio ritiene di dover privilegiare l’interpretazione proposta da una delle sentenze (Sez. 5, n. 22024 del 2013, Carnevale) in cui si era concretizzato il contrasto di giurisprudenza segnalato dalla Sezione rimettente e, in sostanza, fatto proprio dall’ordinanza di rimessione, laddove è stato evidenziato il principio di cui all’art. 1 della legge n. 241 del 1990, in base al quale "l’attività amministrativa persegue fini determinati dalla legge ed è retta da criteri di economicità, efficacia, imparzialità, pubblicità, trasparenza, secondo le modalità previste dalla presente legge e dalle disposizioni che disciplinano singoli procedimenti, nonché dai principi dell’ordinamento comunitario".

8. I principi di cui alla legge n. 241 del 1990 hanno trovato progressive specificazioni nelle disposizioni emanate in tema di organizzazione del pubblico impiego fra le quali assume speciale rilievo la definizione legislativa del "Codice di comportamento" dei dipendenti delle pubbliche amministrazioni ad opera dell’art. 54 d.lgs. 30 marzo 2001, n. 165 (Testo unico sul pubblico impiego), come sostituito dall’art. 1, comma 44, legge 6

novembre 2012, n. 190, e del successivo d.P.R. 16 aprile 2013, n. 62, Regolamento contenente, in attuazione del citato art. 54 del T.U. sul pubblico impiego, il vigente Codice di comportamento dei dipendenti pubblici.

9. I principi cui si è fatto riferimento trovano la loro genesi nelle norme di cui agli artt. 54, 97 e 98 della Costituzione: disposizioni, queste, che chiedono l'adesione del dipendente ai "principi dell'etica pubblica", intesa come locuzione di sintesi dei valori propri della deontologia dell'impiego pubblico, al fine di porre il funzionario nella condizione di servire gli amministrati imparzialmente e con "disciplina ed onore".

La violazione dei doveri d'ufficio, attraverso le varie tipologie di condotta idonee a produrre uno sviamento della prestazione lavorativa dai canoni segnati dalla legislazione di attuazione dei principi di fedeltà ed esclusività del servizio, è stata ripetutamente oggetto della giurisprudenza penale, amministrativa e contabile, che ha posto al centro la prossimità teleologica tra i quei principi, considerati nelle sentenze come espressivi di valori cardine del pubblico impiego, proiezioni del legame tra funzionario e pubblica amministrazione, e tra questa e la comunità degli amministrati.

Si è ritenuto (Sez. U, n. 155 del 29/09/2011, Rossi, dep. 2012, Rv. 251498) che "ai fini della configurabilità del reato di abuso d'ufficio, sussiste il requisito della violazione di legge non solo quando la condotta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti orientata alla sola realizzazione di un interesse collidente con quello per il quale il potere è attribuito, realizzandosi in tale ipotesi il vizio dello sviamento di potere, che integra la violazione di legge poiché lo stesso non viene esercitato secondo lo schema normativo che ne legittima l'attribuzione".

10. Con particolare riferimento all'oggetto specifico della presente decisione vengono in evidenza le norme che regolano la gestione e l'utilizzo dei registri informatizzati dell'amministrazione della giustizia, e, fra questi, il programma Re.Ge. (Registro delle notizie di reato mod. 21), diffuso negli uffici giudiziari, con le conseguenti problematiche di tenuta e sicurezza dei dati.

Il programma Re.Ge., operativo presso ogni Procura della Repubblica, prevede, fino al provvedimento di chiusura dell'indagine preliminare, la sua diretta gestione dalla segreteria del pubblico ministero, cui spetta l'esecuzione dell'iscrizione, disposta dal magistrato ai sensi dell'art. 335 cod. proc. pen., di ogni notizia di reato pervenuta o acquisita di iniziativa "nonché, contestualmente o dal momento in cui risulta, il nome della persona alla quale il reato stesso è attribuito" e dei successivi aggiornamenti, oltre al rilascio delle certificazioni sulle iscrizioni. Queste, non essendo di libera fruibilità per il pubblico, sono circondate dalle limitazioni previste sia dal citato art. 335 (commi 3 e 3-bis) sia dall'art. 110-bis disp. att. cod. proc. pen., secondo il quale: "Quando vi è richiesta di comunicazione delle iscrizioni contenute nel registro delle notizie di reato a norma dell'articolo 335, comma 3, del codice, la segreteria della procura della Repubblica, se la risposta è positiva, e non sussistono gli impedimenti a rispondere di cui all'articolo 335, commi 3 e 3-bis del codice, fornisce le informazioni richieste precedute dalla formula: "Risultano le seguenti iscrizioni suscettibili di comunicazione". In caso contrario, risponde con la formula: "Non risultano iscrizioni suscettibili di comunicazione"".

L'importanza e la delicatezza dell'insieme di iscrizioni nel Re.Ge., delle relative certificazioni e dell'inserimento dei riferimenti ad atti di indagine per ciascun

procedimento giustificano la necessità che il sistema informatico, in quanto registro di cancelleria, sia posto sotto il diretto controllo del procuratore della Repubblica, capo dell'ufficio, nella qualità di responsabile del trattamento e sicurezza dei dati, ai sensi del d.lgs. 30 giugno 2003, n. 196, e di titolare del potere di opporre, se del caso, il segreto investigativo, negando l'accesso ad atti, anche in sede di ispezione o inchiesta dell'Ispettorato Generale del Ministero della giustizia.

11. In ogni caso, l'amministratore dei servizi informatici (ADSI) garantisce che il capo dell'ufficio giudiziario, o un suo delegato, possa accedere alla infrastruttura logistica condivisa per verificare il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri.

Nella materia della tenuta dei registri informatizzati è intervenuto, in sostituzione del d.m. 24 maggio 2001, il d.m. 27 aprile 2009, il quale prevede l'organizzazione centrale e periferica del sistema informatico del Ministero della giustizia, in particolare la D.G.S.I.A. con a capo il Responsabile S.I.A., le strutture interdistrettuali, distrettuali e locali.

All'art. 8 dell'allegato è previsto che venga definita e gestita dal Responsabile S.I.A., con aggiornamenti periodici, la individuazione delle procedure di autenticazione, consistente in generale nella conoscenza di una coppia di informazioni (username e password) per l'accesso, così che ogni utente ottiene, tramite la procedura di autorizzazione, uno specifico insieme di privilegi di accesso ed utilizzo, denominato "profilo di autorizzazione", rispetto alle risorse del sistema informatico. Ogni profilo viene definito in modo tale da assegnare a ciascun utente solo ed esclusivamente i privilegi strettamente necessari per l'espletamento delle attività di propria competenza.

Sono poi stabilite, all'art. 10, le procedure di controllo sulle attività relative all'utilizzo e alla gestione del sistema informatico, sottoposte ad un processo continuo di controllo e verifica a garanzia della autenticità e della integrità dei dati, prevedendosi, come misura minima di monitoraggio, la registrazione di tutti gli accessi, anche di carattere tecnico, ivi compresi quelli non riusciti o falliti, e di tutte le operazioni effettuate sui dati. Controllo che, in virtù del d.lgs. 25 luglio 2006, n. 240, come modificato con legge 22 febbraio 2010, n. 24, compete anche al magistrato capo dell'ufficio giudiziario, per il quale l'art. 1-bis prevede il dovere di assicurare la tempestiva adozione dei programmi per l'informatizzazione predisposti dal Ministero della giustizia per l'organizzazione dei servizi giudiziari, in modo da garantire l'uniformità delle procedure di gestione nonché le attività di monitoraggio e di verifica della qualità e dell'efficienza del servizio.

Il capo dell'ufficio giudiziario è, in definitiva, il responsabile della concreta gestione e del controllo dell'utilizzo dei registri informatizzati secondo i programmi concretamente messi a disposizione dal Ministero della giustizia, che, con le sue strutture, ne garantisce la gestione specificamente tecnica di accesso, controllo e aggiornamento.

12. Le disposizioni normative, di vario livello, sopra esaminate delineano lo status della persona dotata di funzioni pubbliche, il cui agire deve essere indirizzato alle finalità istituzionali in vista delle quali il rapporto funzionale è instaurato: doveri a cui sono correlati i necessari poteri e l'utilizzo di pubbliche risorse, traducendosi in abuso della funzione, nell'eccesso e nello sviamento di potere la condotta che si ponga in contrasto con le predette finalità istituzionali.

Condizioni e doveri che, se connotano in primo luogo la figura del pubblico ufficiale, sia o meno legato all'amministrazione da rapporto organico, ma dotato di poteri autoritativi, deliberativi o certificativi, considerati anche disgiuntamente tra loro, contraddistinguono anche quella dell'incaricato di pubblico servizio, la cui figura è connessa allo svolgimento di un servizio di pubblica utilità presso soggetti pubblici.

E tanto vale anche in riferimento alla gestione dei registri di cancelleria. Ai pubblici dipendenti che, nella loro qualità, debbono operare su registri informatizzati è imposta l'osservanza sia delle diposizioni di accesso, secondo i diversi profili per ciascuno di essi configurati, sia delle disposizioni del capo dell'ufficio sulla gestione dei registri, sia il rispetto del dovere loro imposto dallo statuto personale di eseguire sui sistemi attività che siano in diretta connessione con l'assolvimento della propria funzione. Con la conseguente illiceità ed abusività di qualsiasi comportamento che con tale obiettivo si ponga in contrasto, manifestandosi in tal modo la "ontologica incompatibilità" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estraneo alla ratio del conferimento del relativo potere.

Per converso, il pubblico dipendente, addetto a mansioni d'ordine, cui non possano attribuirsi le qualifiche di pubblico ufficiale o di incaricato di pubblico servizio, che violi le disposizioni del titolare del sistema ed abbia accesso al medesimo al di fuori delle sue mansioni, commette in ogni caso, a prescindere dalle finalità perseguite, il reato di cui al primo comma dell'art. 615-ter cod. pen.

13. Conclusivamente, a fronte del quesito proposto dalla Sezione rimettente, può essere formulato il seguente principio di diritto:

"Integra il delitto previsto dall'art. 615-ter, secondo comma, n. 1, cod. pen. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso (nella specie, Registro delle notizie di reato: Re.Ge.), acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita".

14. L'applicazione di un tale principio di diritto rende evidente la infondatezza del ricorso dell'imputata.

La Corte di appello ha fondato la decisione su una non contestata ricostruzione dei fatti, dando atto che l'indagine di polizia giudiziaria, originata da quella a carico del C. per violazione dell'art. 612-bis cod. pen., aveva accertato i plurimi accessi della S. al Re.Ge., nei termini di cui all'imputazione, ed in particolare le diverse "letture di procedimento" relative all'indagine preliminare a carico del conoscente, assegnata a sostituto procuratore diverso da quello presso il quale svolgeva le sue funzioni. Ha poi osservato che non erano risultati elementi che dimostrassero che quegli accessi e quelle letture fossero state determinate da ragioni di servizio o di interesse pubblico. Ed ha del tutto correttamente sottoposto a critica la motivazione assolutoria del Tribunale, nella parte in cui aveva sostenuto che non si sarebbe potuto escludere "che, nell'ambito di un incarico affidatole da un superiore eventualmente diverso dal (...) titolare del procedimento (...) essa avesse dovuto visualizzare tale fascicolo", trattandosi della formulazione di una mera ipotesi, neppure sostenuta da affermazioni in quel senso della S. .

Con ciò la Corte di merito ha escluso che l’azione della ricorrente fosse stata "coperta" dalla generale autorizzazione ad accedere ai dati di tutti i procedimenti iscritti al Re.Ge., che il Procuratore aggiunto aveva attribuito a tutti i cancellieri ed ai magistrati dell’ufficio, non potendo, all’evidenza, una tale decisione che essere collegata a necessità di servizio, quali rendere più sollecita l’attività dell’ufficio sopperendo a possibili, contingenti, assenze o ad urgenze particolari.

15. È pertanto consequenziale che l’accesso della S. a quei dati si connotasse delle caratteristiche dell’abusività, sicché la Corte di appello ha coerentemente fondato l’affermazione di responsabilità nel rispetto dei principi formulati dalle Sezioni Unite, considerando l’azione della imputata quale operazione non ispirata ai canoni della correttezza e della lealtà, siccome "ontologicamente incompatibile" e diversa rispetto a quelle per le quali, soltanto, la facoltà di accesso le era attribuita.

16. Al rigetto del ricorso consegue la condanna della ricorrente al pagamento delle spese processuali.

P.Q.M.

Rigetta il ricorso e condanna la ricorrente al pagamento delle spese processuali.