Accesso abusivo ad un sistema informatico e sviamento di potere.

Cass. pen., Sez. V, ordinanza 25 gennaio 2017 – 14 marzo 2017, n. 12264, Pres.: Fumo; Rel.: Catena.

I giudici della quinta Sezione penale della Corte di Cassazione, ritenendo di dover superare i principi espressi dalle Sezioni Unite 7 febbraio 2012 n. 4649, sollecitano un nuovo intervento della Corte nella sua massima composizione al fine di stabilire «*se il delitto previsto dall'art. 615 ter c.p., comma 2, n. 1, sia integrato anche dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur 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, e se, quindi, detta condotta, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative, possa integrare l'abuso dei poteri o la violazione dei doveri previsti dall'art. 615 ter c.p., comma 2, n. 1*».

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
LA CORTE SUPREMA DI CASSAZIONE
SEZIONE QUINTA PENALE

Composta dagli Ill.mi Sigg.ri Magistrati:
Dott. FUMO Maurizio - Presidente -
Dott. MAZZITELLI Caterina - Consigliere -
Dott. CATENA Rossella - rel. Consigliere -
Dott. MICHELI Paolo - Consigliere -
Dott. DE MARZO Giuseppe - Consigliere -
ha pronunciato la seguente:

ORDINANZA

sul ricorso proposto da:
S.A.G., nata a (OMISSIS);
avverso la sentenza della Corte di Appello di Milano emessa in data 03/02/2016;
visti gli atti, il provvedimento impugnato ed il ricorso;
udita la relazione svolta dal Consigliere Dott.ssa Rossella Catena;
udito il Pubblico Ministero, in persona del Sostituto Procuratore Generale Dott.ssa Paola Filippi, che ha concluso per il rigetto del ricorso;
udito per la ricorrente l'Avv.to Raffaella Baccaro, in sostituzione del difensore di fiducia Avv.to Dario Celiento, che ha concluso per l'accoglimento del ricorso.

Svolgimento del processo

1. Con la sentenza impugnata la Corte di Appello di Milano, in riforma della sentenza emessa dal Tribunale di Busto Arsizio in data 13/11/201, con cui S.A.G. era stata assolta dai delitti a lei ascritti, la dichiarava colpevole del solo reato di cui al capo A) e la condannava a pena di giustizia.
I capi di imputazione recano la seguente formulazione: A) art. 81 c.p., comma 1, art. 615 ter c.p., comma 1 e comma 2, n. 2 - perchè, con più atti esecutivi di un medesimo disegno criminoso, essendo autorizzata nella propria qualità di cancelliere in servizio presso la Procura della Repubblica di (OMISSIS) 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 nr. (OMISSIS) mod. 21 a carico di C.C., assegnato ad un sostituto procuratore diverso da quello presso cui ella prestava servizio, e relativo ad un suo conoscente, nelle seguenti date ed orari: alle ore 13,37.13 del (OMISSIS); alle ore 16.43.23 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 - B) art. 326 cod. pen. perchè, nella qualità di cancelliere in servizio presso la Procura della Repubblica di (OMISSIS), violando i doveri inerenti alle funzioni o al servizio, avendo acquisito con le modalità meglio indicate nel capo che precede informazioni inerenti il procedimento nr. (OMISSIS) mod.

21, destinate a rimanere segrete, ne rivelava il contenuto a C.C., in particolare informandolo dell'esistenza del procedimento a suo carico; in (OMISSIS), il (OMISSIS).
2. Con ricorso depositato il 22/03/2016 l'imputata, a mezzo del difensore di fiducia Avv.to Dario Celiento, ricorre per violazione di legge e vizio di motivazione, ex art. 606 c.p.p., lett. b) ed e), in relazione all'art. 615 ter c.p.p., affermando che, nel caso in esame, non sarebbe configurabile la condotta tipica prevista dalla norma citata, atteso che la S., cancelliera in servizio presso l'Ufficio di Procura, aveva legittimo accesso al sistema informatico RE.GE., ed atteso altresì che non potrebbe essere ravvisata la volontà contraria da parte del gestore informatico (come rilevabile dalla deposizione del teste M.P., che all'epoca lavorava presso il Tribunale di (OMISSIS) per conto del Ministero della Giustizia, il quale aveva chiarito che tutti i pubblici ministeri ed i soggetti autorizzati, come la ricorrente, avevano accesso indiscriminatamente a tutti i procedimenti iscritti al RE.GE.). In tal senso, peraltro, deponevano anche le disposizioni organizzative interne del Procuratore Aggiunto della Repubblica, che consentivano l'accesso, da parte dei cancellieri abilitati, a tutti i procedimenti iscritti. Nel ricorso si lamenta, altresì, il travisamento della prova, avendo il teste C. inequivocabilmente negato di aver appreso dalla ricorrente di essere iscritto quale indagato per il delitto di cui all'art. 612 bis c.p., notizia, al contrario, appresa dal suo difensore, come dimostrato anche dall'iscrizione ex art. 335 cod. proc. pen., versata in atti, essendo del tutto irrilevante la conoscenza tra il C. e la S., in assenza di seri elementi per ritenere detto teste inattendibile.

Motivi della decisione

Il ricorso va rimesso alle Sezioni Unite, atteso che questo Collegio ritiene, avendo rimeditato lo specifico aspetto evidenziato dal caso in esame, di **doversi discostare dal dictum delle Sezioni Unite, sentenza n. 4649 del 27/10/2011**, dep. il 07/02/2012, Casani ed altri, Rv. 251269, con cui è stato affermato, come è noto, che "Integra il delitto previsto dall'art. 615 ter cod. pen. colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema".
1. Il contrasto rilevato, su cui sono intervenute le Sezioni Unite nel 2011, si fondava su due orientamenti contrapposti, che possono delinearsi in base agli inquadramenti di seguito descritti.
Secondo un primo orientamento di legittimità, risalente a Sez. 5, sentenza n. 12732 del 07/11/2000, dep. 06/12/2000, Zara A., Rv. 217743, si riteneva che il reato di cui all'art. 615 ter cod. pen. potesse essere integrato dalla condotta del soggetto che, essendo abilitato ad accedere al sistema informatico o telematico, lo utilizzasse per finalità diverse da quelle consentite; detta soluzione era motivata in base alla constatata analogia con la fattispecie della violazione di domicilio, per cui si era affermato che la fattispecie criminosa fosse integrata anche dalla condotta di chi, autorizzato all'accesso al sistema informatico per una determinata finalità, utilizzasse il titolo di legittimazione per una finalità diversa e, quindi, non rispettasse le condizioni alle quali era subordinato l'accesso; ne conseguiva, secondo detto orientamento, che se l'accesso richiedeva un'autorizzazione e questa era destinata ad un determinato scopo, la sua utilizzazione per uno scopo diverso non poteva non considerarsi abusiva.
Inoltre, veniva rilevato che la norma in esame puniva non soltanto l'abusivo accesso a sistema informatico, ma anche la condotta di chi vi si mantenesse contro la volontà espressa o tacita di colui che aveva il diritto di escluderlo, con la conseguenza che, qualora il titolo di legittimazione all'accesso venisse utilizzato dall'agente per finalità diverse da quelle consentite, doveva ritenersi che la permanenza nel sistema avvenisse contro la volontà, che poteva anche essere tacita, del titolare del diritto di esclusione.
Pertanto, secondo tale filone interpretativo, commetteva reato anche chi, dopo essere entrato legittimamente in un sistema, continuasse ad operare o a servirsi di esso oltre i limiti prefissati dal titolare; in tale ipotesi ciò che si puniva era l'uso dell'elaboratore avvenuto con modalità non consentite, più che l'accesso ad esso. Coerente con detta impostazione, inoltre, risultava l'art. 615 ter c.p., comma 2, che induceva a ritenere censurabile la condotta del pubblico ufficiale estrinsecantesi in un abuso dei poteri conferitigli, e segnatamente nell'accesso per scopi non istituzionali.
Nel solco di detta pronuncia si erano poi collocate, affrontando specifici aspetti che la condotta dell'agente può assumere nel compimento dell'accesso abusivo: Sez. 2, sentenza n. 30663 del 4/5/2006, G.F., n.m.; Sez. 5, n. 37322 del 08/07/2008, P.C. in proc. Bassani e altro, Rv. 241202; Sez. 5, sentenza n. 1727 del 30/09/2008, dep. 16/01/2009, Romano, Rv. 242939 (secondo cui l'accesso abusivo ad un sistema

informatico, di cui all'art. 615 ter c.p., comma 1, e l'accesso commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri o con abuso della qualità di operatore del sistema, di cui all'art. 615 ter c.p., comma 2, n. 1, configurano due distinte ipotesi di reato, l'applicabilità di una delle quali esclude l'altra secondo il principio di specialità; detta pronuncia è rimasta del tutto isolata); Sez. 5, n. 18006 del 13/02/2009, dep. 30/04/2009, Russo e altri, Rv. 243602; Sez. 5, n. 2987 del 10/12/2009, dep. 22/01/2010, Matassich e altri, Rv. 245842; Sez. 5, n. 19463 del 16/02/2010, Jovanovic, Rv. 247144; Sez. 5, n. 39620 del 22/09/2010, P. G. in proc. Lesce, Rv. 248653.

2. Il secondo orientamento manifestatosi nella giurisprudenza di legittimità, al contrario di quello sin qui esaminato, escludeva che il reato di cui all'art. 615 ter cod. pen. fosse integrato dalla condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne fosse avvalso per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità fossero state effettivamente realizzate. In tal senso era stato osservato che la sussistenza della volontà contraria dell'avente diritto, cui fa riferimento l'art. 615 ter cod. pen., debba 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, quali 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 stesso.

In tal senso si era espressa Sez. 5, n. 2534 del 20/12/2007, dep. 17/01/2008, P.M. in proc. Migliazzo e altri, Rv. 239105; Sez. 5, sentenza n. 26797 del 29/05/2008, Scimia e altri, Rv. 240497; Sez. 6, sentenza n. 39290 dell'08/10/2008, Peparaio, Rv. 242684; Sez. 5, sentenza n. 40078 del 25/06/2009, P.M. in proc. Genchi, Rv. 244749.

3. Le Sezioni Unite Casani, come noto, investite del contrasto, hanno aderito all'orientamento restrittivo da ultimo illustrato, con le argomentazioni contenute nel seguente passaggio motivazionale:

"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 del titolare in ordine all'uso del sistema. Irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuovi 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; sicchè 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 foci 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".

4. In epoca successiva al citato arresto delle Sezioni Unite, le sezioni semplici sono più volte ritornate sulla questione di diritto esaminata. Ad esempio, la Sez. 5, sentenza n. 15054 del 22/02/2012, Crescenzi ed altro, Rv. 252479, ha confermato che ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico, nel caso di soggetto munito di regolare password, è necessario accertare il superamento, su un piano oggettivo, dei limiti e, pertanto, la violazione delle prescrizioni relative all'accesso ed al trattenimento nel sistema informatico, contenute in disposizioni organizzative impartite dal titolare dello stesso, indipendentemente dalle finalità soggettivamente perseguite.
L'orientamento decritto è stato poi ulteriormente approfondito da Sez. 5, sentenza n. 44390 del 20/06/2014, Mecca, Rv. 260763, che ha puntualizzato come, ai fini della configurabilità del delitto in esame, l'accesso di soggetto abilitato debba essere considerato abusivo solo quando l'agente violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, ovvero ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso è a lui consentito.
Nello stesso solco si collocano, inoltre, Sez. 5, sentenza n. 10083 del 31/10/2014, dep. 10/03/2015, Gorziglia ed altro, Rv. 263454; Sez. 5, sentenza n. 44403 del 26/06/2015, Morisco, Rv. 266088; Sez. 5, sentenza n. 33311 del 13/06/2016, Salvatorelli, Rv. 267403.
5. Fatta questa premessa metodologico-ricostruttiva, non vi è alcun dubbio che nel caso in esame la ricorrente potesse legittimamente accedere al sistema RE.GE., in quanto cancelliera in servizio presso la Procura della Repubblica del Tribunale di (OMISSIS), a tanto legittimata da disposizioni interne che rendevano possibile l'accesso al sistema stesso da parte di tutti i soggetti abilitati in maniera indifferenziata, con la possibilità, per il personale amministrativo, ed in particolare per i cancellieri, di accedere, non solo ai procedimenti assegnati al pubblico ministero presso la cui segreteria prestavano servizio, ma anche ed indistintamente a tutti i procedimenti iscritti, per ragioni di carattere organizzativo. Altrettanto indubbia appare la circostanza che la ricorrente non avesse adottato una condotta "abusiva", nel senso di utilizzare password scadute, ovvero password assegnate ad altri funzionari, nè avesse simulato la ricerca attraverso procedimenti inesistenti, o altri simili accorgimenti.
Ciò che tuttavia appare evidente è che la ricorrente avesse effettuato l'accesso al sistema in violazione di normative non regolamentari, ma, ancor prima, di livello legislativo, ossia quelle concernenti il vincolo di fedeltà cui sono tenuti indistintamente tutti i pubblici dipendenti, oltre che in violazione dell'interesse al corretto funzionamento ed all'imparzialità della pubblica amministrazione, apparendo evidente che - pur prescindendo dalla finalità per la quale l'accesso aveva avuto luogo - lo stesso era stato certamente eseguito non in esecuzione di una attività di ufficio. Non può essere dimenticata, infatti, la considerazione che, nella fase delle indagini preliminari, vige, in relazione al registro delle notizie di reato ed alle iscrizioni che in esso vengono effettuate, un incontestato obbligo di riservatezza, come si evince dalla disciplina dell'art. 335 cod. proc. pen. e da quella dell'art. 110 bis disp. att. cod. proc. pen., per cui il diritto di accesso al sistema informatico è consentito soltanto in caso di richiesta di soggetto interessato o di autorizzazione del pubblico ministero, secondo la procedura regolata dalle norme richiamate.
Appare, quindi, doveroso domandarsi se la violazione di doveri ed obblighi fondamentali, ricavabili dal "sistema", e che connotano l'esercizio di un pubblico impiego, anche prescindendo dalle ragioni specifiche di detta violazione, ed anche se non concretantesi in una o più violazioni di norme specificamente dettate per regolare l'accesso al mezzo informatico, possa integrare il delitto di cui all'art. 615 ter cod. pen..
Non appare, infatti, revocabile in dubbio che la norma di cui all'art. 615 ter cod. pen., tuteli interessi molteplici e variegati, rilevanti non solo a livello patrimoniale - come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo - ma anche a livello pubblicistico - quali il diritto alla riservatezza, i diritti afferenti alla sfera militare, sanitaria, quelli inerenti all'ordine pubblico ed alla sicurezza e, tra essi, anche quello al corretto funzionamento dell'amministrazione giudiziaria.
Altrettanto indiscusso può essere ritenuto il rilievo che detti interessi possano essere compromessi da intrusioni o manomissioni non autorizzate, e che in funzione di detta tutela sia previsto uno ius excludendi.
Risulta, pertanto, necessario interrogarsi sul se una interpretazione della norma che faccia coincidere il concetto di autorizzazione unicamente con il rispetto di norme regolamentari ovvero di tipo organizzativo, ritenendo, al contrario, irrilevante la condotta di chi violi - pur attenendosi formalmente alle norme regolamentari specifiche - doveri ben più rilevanti - quali quelli funzionali alla tutela dei predetti interessi pubblicistici (ad esempio: il dovere di fedeltà e di regolarità dell'azione amministrativa cui sono tenuti i pubblici dipendenti), non sia irragionevole dal punto di vista interpretativo, lasciando prive di sanzioni tutte

quelle condotte formalmente osservanti di regole e prassi operative ma che, nel concreto, costituiscono un vero e proprio abuso o eccesso di potere, posto che - come nel caso in esame - chiaramente l'accesso al RE.GE. non era avvenuto in esecuzione di un'attività di ufficio.

6. Proprio su tale base argomentativa, d'altra parte, è iniziata la progressiva "erosione", mediante successive precisazioni e specificazioni da parte di questa Quinta Sezione, del dictum delle Sezioni Unite.

Ed invero, con la sentenza della sez. 5, n. 15054 del 22/02/2012, Crescenzi ed altro, Rv. 252479, è stato affermato che ai fini della sussistenza del reato "ciò che rileva è, quindi, il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che non può ritenersi autorizzato ad accedervi ed a permanervi sia quando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, sia quando ponga in essere operazioni ontologicamente diverse da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito. Il dissenso del dominus loci non viene, quindi, desunto dalla finalità che anima la condotta dell'agente, bensì dalla oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema".

Ancora più specificamente, Sez. 5, sentenza n. 10083 del 31/10/2014, dep. 10/03/2015, Gorziglia ed altro, Rv. 263454, ha affermato che "Ai fini della configurabilità del delitto di accesso abusivo ad un sistema informatico, nel caso di soggetto autorizzato, quel che rileva è il dato oggettivo dell'accesso e del trattenimento nel sistema informatico violando i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema o ponendo in essere operazioni di natura ontologicamente diversa da quelle di cui egli sia incaricato e per le quali sia, pertanto, consentito l'accesso, con conseguente violazione del titolo legittimante l'accesso, mentre sono irrilevanti le finalità che lo abbiano motivato o che con esso siano perseguite".

Inoltre, in Sez. 5, sentenza n. 6176 del 06/11/2015, dep. 15/02/2016, Russo, n. m., si legge che "invero, correttamente i giudici di merito hanno ravvisato nella fattispecie in esame gli estremi del reato in contestazione. In particolare, hanno accertato che l'odierno ricorrente aveva effettuato ripetuti accessi nel sistema informatico, cui era abilitato, ma per ragioni diverse dalle esigenze di polizia giudiziaria per le quali l'autorizzazione era stata concessa dal gestore dell'impianto".

Analogamente in Sez. 5, sentenza n. 35127 del 19/04/2016, Papa, n.m., viene affermato che "Nel caso di specie, è stato - pacificamente - accertato che l'imputato aveva effettuato ripetuti accessi al sistema informatico in dotazione dell'ufficio di appartenenza, contravvenendo alle prescrizioni che ne disciplinano l'uso, limitandolo al solo, istituzionale, scopo di assumere informazioni per ragioni d'ufficio e non già per finalità ad esse estranee".

Anche Sez. 5, sentenza n. 27883 del 09/02/2016, Leo ed altro, n. m., ha ritenuto sussistente il reato di cui all'art. 615 ter cod. pen. in quanto "E' risultato in via generale dalle sentenze di merito che l'autorizzazione all'accesso concerneva esclusivamente le specifiche ragioni di servizio e comportava espresso divieto di interrogazione del sistema su dati anagrafici e fiscali di soggetti diversi da quelli di loro interesse se non nei casi di effettiva necessità e comunque evidentemente previa autorizzazione da parte del dirigente preposto".

Infine, in Sez. 5, sentenza n. 3818 del 29/09/2016, dep. 25/01/2017, Provenzano, n. m., si legge che "Ai fini dell'integrazione del reato risulta di immediata rilevanza se il soggetto, normalmente abilitato ad accedere nel sistema, abbia o meno operato l'accesso in questione nel rispetto delle prescrizioni che legittimano quell'attività (prescrizioni che, per un ufficiale di p.g., possono trovare presupposto nell'esistenza di indagini in corso o nel disbrigo di accertamenti istituzionali, non certo nella richiesta informale di chi, per quanto investito a sua volta di funzioni pubblicistiche, si rivolga a lui come privato cittadino)".

Di tutta evidenza, quindi, risulta come le sentenze citate abbiano tentato di ampliare la portata della sentenza delle Sezioni Unite richiamata, in quanto risulta palese come si sia delineato un filone giurisprudenziale secondo cui il capoverso dell'art. 615 ter c.p. induce a ritenere censurabile, comunque, la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si estrinsechi in un abuso dei poteri conferitigli, tra cui - evidentemente - quello di accessi non istituzionali, e quindi ponendo in essere una condotta formalmente corretta ma ontologicamente difforme dalle finalità operative di cui egli è incaricato, ricordando che la volontà del titolare del diritto di esclusione può, per disposizione di legge, essere anche tacita.

Invero, a differenza del privato, il pubblico ufficiale o l'incaricato di pubblico servizio deve sempre agire nell'osservanza dei limiti co-essenziali alle finalità del suo mandato pubblicistico. Tale limitazione (metodologica, oltre che finalistica) accompagna (e deve caratterizzare) il suo operato anche nell'utilizzo degli strumenti informatici che egli ha a disposizione per espletare i compiti del suo ufficio.

Conseguentemente ritiene questo Collegio che, **almeno con riferimento ai soggetti di cui sopra (e dunque alla ipotesi di cui al comma 2 n. 1 dell'art. 615 ter cod. pen.) le finalità per le quali essi accedono ad (o**

si trattengono in) un sistema informatico, posto funzionalmente (scilicet: per esigenze di servizio) a loro disposizione, non possano essere considerate ininfluenti ai fini della configurazione del delitto in questione. Ciò in quanto le finalità istituzionali, in vista delle quali i predetti soggetti devono operare, sono, per così dire, "incorporate" nel loro status professionale e non possono essere trascurate e, meno che mai, contraddette.

In altre parole: per il pubblico ufficiale e l'incaricato di pubblico servizio, accanto alle eventuali e contingenti norme che regolamentano, nello specifico, la condotta sul luogo di lavoro (con particolare riferimento all'utilizzo - per quel che qui interessa - del mezzo informatico), sono sempre in vigore le norme (legali, regolamentari, deontologiche) che costituiscono le linee direttrici del loro operare pubblicistico e del loro essere (in tale veste) soggetti pubblici. **E poichè ogni potere pubblico è conferito per il raggiungimento di finalità e obiettivi istituzionali, (si argomenta dall'art. 97 Cost.), sembra a questo Collegio, come premesso, che il pubblico ufficiale o l'incaricato di pubblico servizio che utilizzi strumenti informatici del suo ufficio per finalità non coincidenti con quelle per le quali il predetto uso gli è stato concesso, commetta, per ciò solo, il delitto ex art. 615 ter c.p., comma 2, n. 1 perchè, in tal caso il "tradimento" della predetta finalità istituzionale integra inevitabilmente la rescissione del forte vincolo che deve collegare l'obiettivo da raggiungere col potere conferito, appunto, per tale scopo**. Solo in ciò, d'altra parte, potrebbero consistere, secondo l'opinione di questo Collegio, quelle operazioni di natura "ontologicamente diversa", cui ha fatto, piuttosto genericamente, invero, riferimento la giurisprudenza più volte citata.

7. A ciò si deve aggiungere che due interpretazioni palesemente difformi tra loro, benchè basate sulla identica premessa costituita dal decisum delle Sezioni Unite Casani, risultano dalle seguenti pronunce: con Sez. 5, sentenza n. 22024 del 24/04/2013, Carnevale, Rv. 255387 - avete ad oggetto la condotta di un pubblico dipendente, impiegato della Agenzia delle entrate, che aveva effettuato interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio - è stato affermato che 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, nonchè dai principi dell'ordinamento comunitario. Gli organi dello Stato non possono, ovviamente, che agire secundum legem. Ne consegue che l'esercizio del potere pubblico può certamente essere connotato da discrezionalità, ma mai da arbitrio. Dunque: la PA non ha altri poteri se non quelli conferiti dalla legge (legalità formale). Essa inoltre deve esercitare i suoi poteri in conformità ai contenuti prescritti dalla legge (legalità sostanziale). L'amministrazione, poi, è tenuta, non solo a perseguire i fini determinati dalla legge (legalità-indirizzo), ma anche a operare in conformità alle disposizioni normative stesse (legalità-garanzia). Ebbene, la ontologica incompatibilità dell'accesso al sistema informatico è connaturata a un utilizzo dello stesso fuoriuscente dalla ratio del conferimento del relativo potere. In tal caso, la individuazione del fine per il quale il soggetto ha agito (nel caso in esame: esplorare la posizione tributaria dell'on. P.) non riveste certamente valore e significato in sè (come hanno sancito le sezioni unite), ma può assumere valore sintomatico, nel senso che può contribuire a chiarire se il soggetto abbia agito nell'ambito dei suoi poteri istituzionali, ovvero al di fuori degli stessi.

Si tratta, a ben vedere, di una situazione analoga a quella che può determinarsi per i delitti contro la fede pubblica, con riferimento ai quali, essendo, come è noto, sufficiente il dolo generico, la finalità in concreto perseguita dal falsificatore è irrilevante al fine della integrazione della fattispecie, ma può essere illuminante (sintomatica, appunto) per l'interprete, perchè utile per accertare se il falso sia stato intenzionale (e quindi punibile), ovvero dovuto a ignoranza, superficialità, disattenzione. Ora, non può certo essere dubbio che ciò che conferisce legalità alla attività amministrativa è il fatto di essere rivolta a perseguire l'interesse pubblico, come dettato dall'indirizzo politico. Evidentemente, nessuna norma di legge o regolamentare, nessun ordine e nessuna circolare autorizzava, nel caso di specie, un semplice dipendente dell'Agenzia di Noto a verificare la posizione di contribuenti aventi ben altro domicilio fiscale. Ne consegue che certamente devono ritenersi violate le prescrizioni del dominus foci, vale a dire della competente PA, per violazione del ricordato art. 1 della legge sopra richiamata".

Con sentenza della Sez. 5, n. 44390 del 20/06/2014, Mecca, Rv. 260763, è stato, al contrario, affermato come non fosse possibile "ravvisare l'abusività dell'accesso nella violazione delle regole che presiedono allo svolgimento dell'attività amministrativa, quali sinteticamente enunciate dalla L. 7 agosto 1990, n. 241, art. 7, secondo cui 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, nonchè dai principi dell'ordinamento comunitario. E evidente che il parametro di riferimento è divenuto, per il giudice della cautela, non già il complesso delle disposizioni impartite dal dominus loci, ma il complesso delle disposizioni che regolano e indirizzano l'attività amministrativa verso i fini determinati dalla legge, finendo con l'identificare l'abusività - com'era inevitabile, data la premessa - nella violazione della regola di imparzialità e trasparenza che regge l'azione amministrativa e col frustrare la ratio dell'orientamento a cui - formalmente - ha inteso dare applicazione (evitare una dilatazione del concetto di accesso abusivo oltre i limiti imposti dalla necessità di tutelare i diritti del proprietario del sistema). Nè diverso significato ha il riferimento all'art. 9 della legge istitutiva dello SDI, che individua i soggetti abilitati ad accedere al sistema informatico, ma non detta prescrizioni in ordine alle modalità dell'accesso e alle operazioni consentite all'utente abilitato e, nel vietare ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'art. 6, lett. a), pone un obbligo successivo e ulteriore rispetto a quello che grava sull'utente suddetto".

8. In tal senso, dunque, appare necessario un chiarimento in relazione alla portata del principio fissato dalla decisione di Sez. U. Casani e, per tale ragione, si richiede che il presente ricorso venga rimesso al Supremo Collegio nomofilattico.

In particolare, il profilo controverso è quello individuato dal **quesito se ciò che integra la illiceità dell'accesso da parte di chi è formalmente autorizzato, non sia solo la violazione di disposizioni regolamentari ed organizzative, ma anche lo sviamento del potere, pur in assenza di dette violazioni**.

Ciò del tutto coerentemente con la condotta tipica del delitto di cui all'art. 615 ter c.p., in quanto l'intrusione informatica non necessita della realizzazione di condotte ulteriori, ben potendo sostanziarsi in una semplice lettura dei dati contenuti nel sistema.

Orbene, nel caso di specie, è rimasto accertato, per come è lecito desumere dalla motivazione delle due sentenze di merito, che nel sistema RE.GE. fossero custoditi i dati relativi ai procedimenti penali iscritti presso la Procura della Repubblica di (OMISSIS), di cui la ricorrente era cancelleria, in quanto tale tenuta ad un corretto utilizzo degli strumenti in dotazione dell'Amministrazione di appartenenza e, quindi, anche del sistema informatico, per le finalità tipiche dell'Amministrazione della giustizia. E' del tutto evidente che l'accesso allo specifico procedimento penale non era stato affatto compiuto nell'interesse della detta amministrazione, non essendo in discussione che esso non fosse derivante da una specifica attività di ufficio, e, quindi, che fosse stato attuato con il dissenso (sia pure non espresso, essendo, ovviamente, l'accesso avvenuto clandestinamente) degli organi preposti alla tutela della funzione pubblica, benchè in assenza di qualsivoglia violazione di specifiche regole organizzative.

In realtà, ciò che emerge dalla applicazione concreta del principio affermato dalle Sezioni Unite, è la sussistenza di una ambiguità di fondo nella individuazione pratica e nell'applicazione del principio secondo cui, ai fini dell'integrazione della fattispecie criminosa in questione, non assumono rilievo alcuna gli scopi e le finalità che hanno motivato l'accesso, in quanto, approfondendo l'analisi dello specifico aspetto, va rilevato che l'uso delle informazioni acquisite fatto dall'agente - che rappresenta certamente un elemento estraneo alla fattispecie, inidoneo a delimitarne la portata e, al più, idoneo ad integrare una distinta ipotesi criminosa - è sicuramente concetto diverso dalla finalità che determina l'agente stesso; quest'ultima, infatti, può sicuramente apparire rivelatrice del superamento dei limiti dell'autorizzazione all'accesso al sistema, manifestando un vero e proprio eccesso di potere o sviamento di potere, e, quindi, costituire elemento rilevante ai fini dell'integrazione della fattispecie, come nel caso in esame.

In generale, infatti, la finalità della condotta, intesa come movente di qualsiasi azione umana, sicuramente non rientra nella struttura del reato, tutte le volte in cui non sia richiesto un dolo specifico per la integrazione della fattispecie; nondimeno essa può apparire illuminante ai fini della valutazione della illiceità della condotta stessa. Sotto detto aspetto, quindi, appare necessario distinguere la finalità della condotta, così come essa viene rivelata dalla commissione di una ulteriore attività, integrante una diversa ed autonoma fattispecie di reato, che, in realtà coincide con l'uso che l'agente fa delle informazioni acquisite all'esito dell'accesso abusivo nel sistema informatico, da tenere distinta dalla finalità della condotta rivelata dalle specifiche modalità dell'azione. Nella specie, specularmente, può, anzi, dirsi che proprio la mancanza di una finalità coerente con il legittimo esercizio del potere per motivi di ufficio, da parte dell'agente, appaia rivelatrice del dolo dell'accesso abusivo nel sistema informatico.

D'altra parte non può dimenticarsi come la previsione dell'art. 615 ter c.p., comma 2, individui la sussistenza di una circostanza aggravante rispetto alla previsione generale, che è caratterizzata non solo dalla qualità soggettiva dell'agente - pubblico ufficiale o incaricato di pubblico servizio - ma anche dall'abuso dei poteri.

Il concetto stesso di abuso di potere, infatti, evoca l'uso di un potere che, attribuito al pubblico ufficiale o all'incaricato di pubblico servizio per determinate finalità individuate dalla legge, venga esercitato in maniera non coerente con le predette finalità, ossia si risolva in un eccesso o in uno sviamento nell'esercizio del potere stesso.

Peraltro **non può apparire irrilevante che il legislatore, nell'individuare la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio, ai sensi dell'art. 615 ter c.p., comma 2, n. 1, abbia alternativamente previsto la concretizzazione di detta condotta attraverso l'abuso dei poteri o la violazione dei doveri inerenti la funzione o il servizio**. Appare, cioè, evidente che il legislatore, nel delineare i caratteri salienti della condotta di accesso abusivo ad un sistema informatico o telematico, abbia inteso chiaramente perseguire sia le condotte che si traducano un una palese violazione di un dovere - ossia una condotta che si manifesta ex se illecita nel momento in cui viene posta in essere, la sua stessa attuazione costituendo la violazione di un preciso dovere comportamentale rispetto al quale essa si pone in aperta e diretta violazione - sia le condotte che, formalmente in linea con i poteri attribuiti all'agente, costituiscano, tuttavia, un eccesso o uno sviamento del potere stesso, in quanto la loro manifestazione non risulta coerente con l'interesse pubblico per il raggiungimento del quale l'accesso al sistema è stato autorizzato; dette ultime condotte, infatti, appaiono addirittura più insidiose, oltre che altrettanto lesive, rispetto a quelle attuate in palese violazione di un dovere.

Ne discende, quindi, stante la ravvisata necessità di ulteriormente approfondire il decisum delle Sezioni Unite - alla luce degli illustrati pronunciamenti, successivi alla sentenza Casani, ed alla luce delle considerazioni svolte da questo Collegio la rimessione del ricorso alle Sezioni Unite, sulla base del seguente quesito: "**se il delitto previsto dall'art. 615 ter c.p., comma 2, n. 1, sia integrato anche dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur 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, e se, quindi, detta condotta, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative, possa integrare l'abuso dei poteri o la violazione dei doveri previsti dall'art. 615 ter c.p., comma 2, n. 1**".

P.Q.M.

Rimette il ricorso alle Sezioni Unite.
Così deciso in Roma, il 25 gennaio 2017.
Depositato in Cancelleria il 14 marzo 2017