REPUBBLICA ITALIANA

In nome del Popolo Italiano

14546-17

LA CORTE SUPREMA DI CASSAZIONE

QUINTA SEZIONE PENALE

Composta da

Paolo Antonio Bruno	- Presidente -	Sent. n. sez. 1812
Gerardo Sabeone		CC - 26/10/2016
Sergio Gorjan		R.G. N. 27322/2016
Paolo Micheli	- Relatore -	
Andrea Fidanzia		

ha pronunciato la seguente

SENTENZA

sul ricorso proposto nell'interesse di

(omissis) , nato a (omissis)

(nella qualità di legale rappresentante della (omissis) s.r.l.)

avverso la sentenza emessa il 16/12/2015 dal Gup del Tribunale di Milano all'esito del processo penale celebrato nei confronti di

(omissis) , nato a (omissis)

visti gli atti, la sentenza impugnata ed il ricorso;

udita la relazione svolta dal consigliere Dott. Paolo Micheli;

udito il Pubblico Ministero, in persona del Sostituto Procuratore generale Dott. Giovanni Di Leo, che ha concluso chiedendo il rigetto del ricorso;

udito per la parte civile ricorrente l'Avv. (omissis) , il quale ha concluso chiedendo l'accoglimento del ricorso e l'annullamento della sentenza impugnata;

udito per l'imputato non ricorrente l'Avv. (omissis) , la quale ha concluso chiedendo dichiararsi l'inammissibilità, ovvero il rigetto, del ricorso della parte civile

RITENUTO IN FATTO

1. Con la sentenza indicata in epigrafe, il Gup del Tribunale di Milano dichiarava non luogo a procedere nei confronti di (omissis), imputato in ordine al delitto di cui all'art. 615-*ter*, commi 1 e 2, cod. pen.: il giudicante riteneva non sussistente il fatto-reato addebitato all'imputato, consistito nell'essersi, quale dipendente della (omissis) s.r.l., intrattenuto indebitamente nel sistema informatico-telematico della suddetta società, tramite un *account* aziendale di cui era titolare, in particolare inviando dalla casella di posta elettronica correlata al medesimo *account* tre comunicazioni ad indirizzi esterni, con allegati un *data-base* relativo all'intero *know how* della (omissis), un *file* contenente il fatturato dei principali editori della società ed un ulteriore documento concernente il fatturato di altra azienda verso alcuni clienti della stessa (omissis).

Ad avviso del giudicante, nella vicenda in esame non potevano trovare applicazione i principi affermati dalle Sezioni Unite di questa Corte con la decisione n. 4694/2012 del 27/10/2011 (ric. Casani), dato che quel precedente non riguardava il peculiare caso di una semplice spedizione di *e-mail*: in particolare, una simile ipotesi non poteva essere intesa quale modalità della condotta di "mantenersi" all'interno di un sistema informatico, prevista dalla norma incriminatrice e tale da richiedere un tempo apprezzabile per acquisire una dimensione offensiva autonoma, risolvendosi invece in un'operazione istantanea di sola pressione su un tasto di invio. Inoltre, pur essendo pacifico che l'imputato non avesse osservato una prescrizione impartita dai dirigenti dell'azienda (nel contratto di assunzione era stato stabilito il divieto di utilizzare, per l'invio di documenti di lavoro riservati e/o afferenti il *know how* della (omissis) s.r.l., la casella di posta elettronica a lui assegnata), il (omissis) aveva agito nell'esercizio delle mansioni che gli erano state affidate e con operazioni coerenti alle medesime, senza dunque alcun radicale sovvertimento delle regole preposte al funzionamento del sistema informatico *de quo*.

2. Avverso la pronuncia del Gup milanese propone ricorso per cassazione, anche agli effetti penali, il difensore / procuratore speciale nominato dal legale rappresentante della (omissis) s.r.l., già costituita parte civile. Nell'atto di impugnazione si passano preliminarmente in rassegna le scansioni del procedimento: il ricorrente ricorda come il fatto sia stato accertato in termini assolutamente pacifici, e che a seguito della contestazione e della successiva querela il P.M. si limitò a prendere atto della versione offerta dall'indagato in sede di interrogatorio, formalizzando una richiesta di archiviazione poi non

accolta dal Gip. In quella prima ordinanza, del 27/09/2015, dove il giudicante richiamò la pronuncia delle Sezioni Unite già menzionata, si legge che «nella presente fattispecie paiono sussistere tutti gli elementi costitutivi del delitto di cui all'art. 615-*ter* cod. pen., in quanto l'autorizzazione ad entrare e ad utilizzare il sistema informatico escludeva la possibilità di inviare ad altro sistema informatico i dati, ovvero trasferirli su supporti mobili».

2.1 La difesa della parte civile deduce quindi erronea applicazione della norma incriminatrice. Vero è che il caso di un invio di posta elettronica non venne affrontato dalle Sezioni Unite nel 2011, ma solo perché quella fattispecie concreta era del tutto diversa; *ergo*, i principi affermati nella sentenza Casani - di cui il ricorrente richiama diffusamente le argomentazioni - debbono senz'altro valere anche nella fattispecie odierna. Ciò comporta che fra le condotte sanzionate deve ritenersi contemplata anche quella di «mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha diritto di esclusione, da intendersi come il persistere nella già avvenuta introduzione, inizialmente autorizzata o casuale, violando le disposizioni, i limiti e i divieti posti dal titolare del sistema»

2.2 Sul concetto di "mantenersi" di cui al precetto disegnato dall'art. 615-*ter* cod. pen., inoltre, il difensore del (omissis) individua un ulteriore profilo di violazione di legge: la norma, infatti, descrive una ipotesi di reato di mera condotta, non già permanente (ed è pertanto erroneo il parallelo, illustrato dal giudice di merito, con il delitto di sequestro di persona e con le sue implicazioni in ordine al tempo di apprezzabile durata che ne costituisce il presupposto). A riguardo, nel ricorso viene evocata una diversa pronuncia delle Sezioni Unite (la sentenza n. 17325 del 26/03/2015, relativa ad un conflitto di competenza in tema di individuazione del *locus commissi delicti* in caso di accesso abusivo ad un sistema informatico o telematico), e si fa comunque presente che anche chi si limita a digitare sulla tastiera di un *computer* il pulsante di invio - per una comunicazione *e-mail* - deve intendersi aver compiuto tutta una serie di attività preliminari certamente idonee ad integrare la condotta di "mantenersi" nel sistema. Ciò in quanto il comportamento *de quo* deve leggersi in senso informatico, piuttosto che in termini strettamente materiali.

2.3 Infine, il ricorrente si duole dell'inosservanza ed erronea applicazione del citato art. 615-*ter*, nonché della contraddittorietà della motivazione della sentenza impugnata, nella parte in cui il giudicante reputa necessario - ai fini della ravvisabilità del reato - un radicale sovvertimento delle regole poste a tutela del sistema: al contrario, la tesi della difesa di parte civile è che sia sufficiente rilevare il mancato rispetto di disposizioni specifiche, purché queste risultino essere state certamente impartite e recepite come coessenziali alla disciplina dettata dal *dominus loci* per la gestione del sistema medesimo. La

difesa di parte civile, in particolare, reputa «irrilevante che i dati potevano essere trattati dal signor (omissis), ed acquista invece estrema (penale) rilevanza il fatto che li abbia trattati attraverso un metodo telematico/informatico che era espressamente vietato, con ciò perfezionando l'elemento oggettivo del reato in questione.

Del resto, anche per giungere alle conclusioni date per scontate dal Gup (secondo cui il (omissis) avrebbe compiuto operazioni sempre coerenti alle mansioni che gli erano state affidate all'interno della (omissis)) sarebbe stato comunque necessario assumere prove documentali e/o testimoniali, così rendendosi evidente *in re ipsa* l'imprescindibilità di un approfondimento dibattimentale.

3. In data 05/10/2016, il difensore dell'imputato ha depositato una memoria con la quale mira a confutare le argomentazioni della controparte privata. Premesso che il fatto materiale, concretamente realizzato dal (omissis), fu quello di inviare, dal *personal computer* aziendale, tre documenti ad un suo indirizzo personale di posta elettronica, la difesa segnala che «non è mai stato posto in dubbio [...] che il (omissis) fosse autorizzato ad accedere ed utilizzare il sistema informatico, che potesse prendere cognizione e copiare tutti i dati ivi contenuti e, altresì, utilizzare la posta elettronica. Il divieto era relativo solo all'invio di alcuni *file*, ossia quelli contenenti *know how*, attraverso la posta della società, per evitare che terzi la potessero intercettare». Perciò, quella che viene addebitata all'imputato non è una condotta di introduzione o di mantenimento nel sistema, uniche ipotesi sanzionate dal legislatore, bensì una modalità di impiego successivo di dati legittimamente acquisiti; con la conseguenza che il Gup, «dato atto che il (omissis), nell'ambito delle più ampie mansioni a cui era adibito, poteva accedere ed intrattenersi senza limiti nel sistema della società e prendere cognizione, salvare, copiare tutti i dati e le informazioni ivi contenute, che pertanto non vi fosse abusivo intrattenimento né con riferimento alle prescrizioni della società, né con riferimento all'attività da lui svolta, ha correttamente ritenuto, proprio alla luce della giurisprudenza richiamata dalla parte civile, che il reato non sussiste».

CONSIDERATO IN DIRITTO

1. Il ricorso è meritevole di accoglimento.

1.1 Deve innanzi tutto ricordarsi che, secondo la giurisprudenza di questa Corte, il Giudice dell'udienza preliminare è chiamato a pronunciare una decisione liberatoria - anche nelle ipotesi di cui all'art. 425, comma 3, del codice di rito -

«se gli elementi acquisiti risultino insufficienti, contraddittori o comunque non idonei a sostenere l'accusa in giudizio, non potendo procedere a valutazioni di merito del materiale probatorio ed esprimere, quindi, un giudizio di colpevolezza dell'imputato ed essendogli inibito il proscioglimento in tutti i casi in cui le fonti di prova si prestino a soluzioni alternative e aperte o, comunque, ad essere diversamente rivalutate» (Cass., Sez. II, n. 48831 del 14/11/2013, Maida, Rv 257645). Più di recente, si è precisato che «in sede di legittimità, il controllo sulla motivazione della sentenza di non luogo a procedere non deve incentrarsi su distinzioni astratte tra valutazioni processuali e valutazioni di merito, ma deve avere riguardo - come per le decisioni emesse all'esito del dibattimento - alla completezza ed alla congruità della motivazione stessa, in relazione all'apprezzamento, sempre necessario da parte del Gup, dell'aspetto prognostico dell'insostenibilità dell'accusa in giudizio, sotto il profilo della insuscettibilità del compendio probatorio a subire mutamenti nella fase dibattimentale» (Cass., Sez. VI, n. 29156 del 03/06/2015, Arvonio, Rv 264053).

1.2 Tanto precisato, nella fattispecie concreta non può che rilevarsi una diversa prospettazione - della parte civile, da un lato, e dell'imputato, dall'altra - circa l'effettiva estensione delle facoltà spettanti al (omissis), nell'esercizio delle mansioni correlate alla sua attività lavorativa. Secondo il difensore del prevenuto, egli aveva titolo a fare copia di qualunque *file*, con l'unico limite di non poter utilizzare la posta elettronica per l'invio di documenti contenenti dati sensibili o riservati; la parte civile, invece, censura la sentenza impugnata anche laddove il giudicante si sofferma sulla stessa consistenza materiale di un'attività di comunicazione via *e-mail* (per escludere che questa concretizzi una condotta di "mantenimento", rilevante *ex* art. 615-*ter* cod. pen.), segnalando a pag. 18 dell'odierno ricorso che «se si dovesse aderire alle tesi del Gup, la copiatura di un *file* su una chiavetta (oggi possibile utilizzando il comando "invia a" attraverso la semplice digitazione del tasto destro del *mouse*) sarebbe una condotta perfettamente lecita anche se posta contro la volontà del titolare del sistema informatico». Già in precedenza, peraltro, la parte ricorrente aveva richiamato le argomentazioni esposte dal Gip con il provvedimento reiettivo dell'iniziale richiesta di archiviazione, secondo cui il (omissis) era certamente abilitato ad accedere ed a trattenersi nel sistema *de quo*, ma «l'autorizzazione ad entrare e ad utilizzare il sistema informatico» non escludeva solo «la possibilità di inviare ad altro sistema informatico i dati», non contemplando parimenti la possibilità di «trasferirli su supporti mobili» (v. pag. 7 dell'atto di impugnazione).

Tale aspetto, in definitiva, risultava e risulta ancora non chiarito, dovendosi pertanto ritenere in linea di principio indefettibile la celebrazione di un giudizio dibattimentale per verificare se il (omissis) agì - al di là dell'essere venuto meno

ad una *policy* dettata per soli fini di tutela della riservatezza dei dati - non osservando una prescrizione coessenziale alla stessa legittimità dell'accesso di cui si discute.

1.3 La giurisprudenza delle Sezioni Unite di questa Corte, del resto, ha avuto modo di affermare 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» (Cass., Sez. U, n. 4694/2012 del 27/10/2011, Casani, Rv 251269).

Al massimo organo di nomofilachia, nell'occasione, era stato proposto il quesito "se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o 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"; nello sviluppo motivazionale della decisione, dopo aver dato atto del contrasto interpretativo, le Sezioni Unite segnalavano come 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 (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». Ne deriva, secondo l'insegnamento che può trarsi dalla sentenza Casani, che «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.)».

Ergo, ai fini dell'integrazione del reato risulta decisivo comprendere se un soggetto, ove normalmente abilitato ad accedere nel sistema oggetto di verifica, vi si sia introdotto rispettando o meno le prescrizioni costituenti il presupposto legittimante l'attività in questione: ed è fisiologico che, per un peculiare "domicilio informatico", il *dominus loci* possa apprestare le regole che ritenga più opportune per disciplinare l'accesso e le conseguenti modalità operative (ivi compresa la possibilità di mantenersi all'interno del sistema copiando un *file* od inviandolo a mezzo posta elettronica, incombenza che non si esaurisce nella mera pressione di un tasto ma è piuttosto caratterizzata da una apprezzabile dimensione cronologica). Nell'ambito di una data azienda, in definitiva, ben potrebbe darsi che siano poste regole di accesso e mantenimento nel sistema che il *management* di un'altra società consideri invece del tutto irrilevanti.

2. Si impongono, pertanto, le determinazioni di cui al dispositivo.

P. Q. M.

Annulla la sentenza impugnata, con rinvio al Tribunale di Milano, ufficio del Giudice dell'udienza preliminare, per nuovo esame.

Così deciso il 26/10/2016.

Il Consigliere estensore
Paolo Micheli

Il Presidente
Paolo Antonio Bruno

DEPOSITATA IN CANCELLERIA
oggi 24 MAR 2017
IL FUNZIONARIO GIUDIZIARIO
Cosimo Lanzone