Corte di Cassazione

Sez. V Penale, sentenza n. 10083 del 31 ottobre 2014 – 10 marzo 2015

Ritenuto in fatto

1. Con sentenza del 18 novembre 2013 la Corte d'appello di Milano ha confermato la pronunzia emessa in primo grado dal Tribunale della stessa città nei confronti di G.G. , ritenuto responsabile del reato di cui agli articoli 615-ter, comma secondo, nn. 1 e 3, 81 capoverso e 61 n. 7 cod. pen., "perché, in qualità di socio e consigliere di amministrazione della MIDA s.r.l. e, in forza di tale qualità, in possesso delle credenziali di accesso alle banche dati aziendali, da qualificarsi quale operatore del sistema, in tempi diversi ed in esecuzione del medesimo disegno criminoso:
- in seguito alla comunicazione dell'interruzione del rapporto di collaborazione comunicata e ricevuta in data 31 marzo 2008, ancorché ancora in possesso delle credenziali personali, accedeva e si manteneva abusivamente sul sistema informatico della MIDA s.r.l., protetto da sistemi di sicurezza, visualizzando file contenenti i dati riguardanti l'attività dell'azienda;
- in data 6 aprile 2008 duplicava su supporto ottico numerosi file contenuti nella banca dati aziendale e riguardanti clienti dell'azienda, sfruttando le informazioni acquisite per fare disdire ai clienti diverse polizze assicurative contratte presso la MIDA s.r.l., causando un danno economico alla MIDA s.r.l., che la stessa ha quantificato per la somma di circa Euro 794.298,84 e, successivamente, effettuava l'eliminazione di file a carattere professionale contenuti nell'hard disk del computer in uso e di proprietà dell'azienda (reato commesso in Milano nell'aprile 2008)".
Con la pronunzia di primo grado l'imputato oltre ad essere stato condannato alla pena di giustizia, applicate le circostanze attenuanti generiche equivalenti alla contestata aggravante, era stato condannato anche al risarcimento dei danni in favore della parte civile costituita, da liquidarsi in separata sede, nonché al pagamento di una provvisionale nella misura di Euro 30.000.
2. Propone ricorso l'imputato, deducendo i seguenti tre motivi.
2.1. Violazione di legge con riferimento a norme processuali di cui agli articoli 507, 523, 526, 604 cod. proc. pen..
La Corte territoriale ha rigettato il primo motivo di appello presentato dall'imputato sul presupposto dell'assoluta legittimità dell'acquisizione della copia del codice deontologico sottoscritto dallo stesso imputato e posto a fondamento della sentenza di condanna di primo grado. Tale documento era stato prodotto dalla parte civile costituita in giudizio solo dopo la chiusura del dibattimento e, peraltro, successivamente anche alla formulazione delle richieste della pubblica accusa.
Rileva il ricorrente che l'articolo 526 cod. proc. pen. non si limita a stabilire le modalità secondo cui va deliberata la decisione, ma risolve negativamente il quesito se una certa prova possa entrare nel patrimonio cognitivo del giudice destinato a fungere da base per la formazione del convincimento. La norma, nel momento in cui prescrive l'inutilizzabilità delle prove diverse da quelle legittimamente acquisite nel dibattimento, impedisce al giudice di avvalersene. Ne consegue che, posto l'intimo collegamento funzionale tra la prova acquisita e la sentenza, una volta escluso che questa possa fondarsi sulle prove inutilizzabili, è da ritenersi irrimediabilmente nulla e deve trovare applicazione il disposto di cui all'articolo 604, comma 4, cod. proc. pen., che però - secondo il ricorrente - non è stata rispettato nel caso di specie.
Rappresenta altresì che il codice deontologico, nella versione da lui firmata, ha costituito elemento di prova per affermare la sua responsabilità penale. Tale documento però è stato acquisito dopo la chiusura dell'istruttoria dibattimentale e non è mai stato oggetto di specifiche precedenti contestazioni, nemmeno nel corso dell'esame dell'imputato. La Corte territoriale, per superare l'eccezione sollevata con il motivo di appello, ha affermato che: "la sussistenza di tale disposizione non è in contestazione e data la qualità dell'imputato all'interno della società deve ritenersi pacifico che la conoscesse". In tal modo il giudice di secondo grado - secondo il ricorrente - ha trasformato una prova rilevante e posta a fondamento della condanna di primo grado, in un elemento "irrilevante ai fini della decisione". Il ricorrente eccepisce quindi la inutilizzabilità del codice deontologico con la propria firma apposta in calce, depositato successivamente alla chiusura del dibattimento dalla parte civile.
2.2. Violazione dell'articolo 606, lettera e, cod. proc. pen. per mancanza di motivazione ed illogicità della sentenza in merito alla ritenuta responsabilità dell'imputato.

Il ricorrente rileva che la Corte territoriale è incorsa in un palese travisamento della prova, dando per certi fatti in alcun modo dimostrati. Il codice deontologico prodotto e richiamato in atti infatti non esclude ex se né la copia né la duplicazione dei file, stabilendo invece un divieto solo a fronte di una copia "*finalizzata a qualcosa di diverso dal consentito*", lasciando pertanto lecita la condotta in senso oggettivo. Secondo il ricorrente né il giudice di primo grado né quello di appello si sono preoccupati di descrivere i motivi o il percorso logico che abbia permesso di individuare in primo luogo cosa è stato copiato e, successivamente, le intenzioni dell'imputato al momento del fatto (esattamente ciò che secondo il codice deontologico è rilevante ai fini della preventiva autorizzazione), nonché in ogni caso le prove da cui sarebbe emersa in concreto la finalità e, quindi, la non autorizzazione al compimento di tali copie.
Peraltro, rileva il ricorrente, i giudici di merito hanno ritenuto scontato che tali copie fossero state fisicamente portate all'esterno della società, senza spiegare né quando né come né in base a quali prove ciò sia stato dedotto, perché l'unica cosa certa emersa in dibattimento è che è stata fatta una copia di file non meglio individuati, in un tempo in cui l'imputato era ancora pacificamente pienamente operativo nelle sue mansioni all'interno della società.
2.3. Con il terzo ed ultimo motivo il ricorrente deduce l'omessa motivazione e la illogicità della sentenza in merito alla condanna al risarcimento del danno, oltre che al riconoscimento della provvisionale in favore della parte civile.
I giudici di merito - secondo il ricorrente - hanno compiuto una deduzione logica palesemente forzata ritenendo esistente il danno patrimoniale sulla base del solo elemento temporale, secondo cui i clienti persi dalla MIDA s.r.l. sarebbero poi passati rapidamente alla ESEDRA, nuova società nella quale l'imputato è andato a lavorare.
Il ricorrente ha quindi dedotto che il giudice del lavoro che si era occupato della stessa vicenda aveva escluso con sentenza, prodotta in sede di appello, che ci fosse un nesso causale tra la nuova attività lavorativa dell'imputato e il lamentato pregiudizio patrimoniale della MIDA s.r.l., ritenendo che non vi fosse alcun collegamento tra l'avvenuta copiatura dei dati aziendali contenenti gli elenchi della clientela e le disdette della stessa clientela.
Di tali circostanze la Corte territoriale non ha tenuto minimamente conto e non ha dato rilievo alla scelta della parte civile di rinunciare ai propri testimoni, unici soggetti che avrebbero potuto fornire eventualmente la prova del nesso causale esistente tra la condotta contestata all'imputato e la perdita di clienti da parte della MIDA s.r.l.

Considerato in diritto

Il ricorso è fondato e va accolto nei termini qui di seguito precisati.
1. Il primo motivo di ricorso non appare meritevole di accoglimento, ove si consideri che lo stesso ricorrente finisce per non contestare il contenuto della disposizione del codice deontologico utilizzata per la decisione dai giudici di merito, di cui una copia non firmata era stata legittimamente già acquisita durante l'istruttoria dibattimentale, sicché irrilevante è la questione in ordine alla utilizzabilità o meno ai fini della decisione del documento prodotto tardivamente dalla parte civile solo in sede di discussione.
2. Vanno invece accolte le doglianze mosse dal G. con gli altri due motivi di ricorso.
In punto di diritto si deve premettere che ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico (art. 615 ter cod. pen.), 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 (Sez. 5, n. 15054 del 22/02/2012 - dep. 18/04/2012, Crescenzi e altro, Rv. 252479).
È noto che in ordine all'interpretazione di tale norma vi è stato un contrasto della giurisprudenza di legittimità e di merito.
Secondo un orientamento (ex multis, Sez. 5, n. 12732 del 7 novembre 2000, Zara; Sez. 5, n. 37322 in data 8 luglio 2008, Bassani; Sez. 5, n. 1727 del 30 settembre 2008, Romano) integra la fattispecie di accesso abusivo ad un sistema informatico non solo la condotta di chi vi si introduca essendo privo di codice di accesso, ma anche quella di 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; insomma l'utilizzazione dell'autorizzazione per uno

scopo diverso non potrebbe non considerarsi abusiva.
Un diverso orientamento (Sez. 5, n. 2534 dei 20 dicembre 2007, Migliazzo; Sez. 5, n. 26797 del 29 maggio 2008, Scimmia; Sez. 6, n. 3290 in data 8 ottobre 2008, Peparaio) aveva, invece, valorizzato il dettato della prima parte dell'art. 615 ter ed aveva ritenuto illecito il solo accesso abusivo, mentre sempre e comunque lecito considerava l'accesso del soggetto abilitato, ancorché effettuato per finalità estranee a quelle dell'ufficio e perfino illecite.
Le Sezioni Unite della Suprema Corte (S.U., n. 4694/12 del 27 ottobre 2011, Casani) nel comporre il contrasto hanno sottolineato che la questione non può 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 nel sistema informatico. 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.
Non appare a questo punto superfluo richiamare il passaggio saliente della motivazione di tale pronunzia e verificare l'applicazione che in concreto del principio affermato hanno fatto le Sezioni Unite.
La sentenza evidenzia che rilevante deve ritenersi 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 c.p.).
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.
Soprattutto da quest'ultimo passaggio della motivazione emerge chiaramente l'effettiva estensione del principio affermato dalle Sezioni Unite, che, infatti, nell'applicarlo hanno ritenuto configurabile il reato ex art. 615 ter cod. pen. in una fattispecie in cui un carabiniere aveva consultato lo SDI per esigenze diverse da quelle di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione dei reati per cui era stato legittimato ad operare sul sistema. Nell'occasione la Corte

non ha coerentemente preso in considerazione le finalità per cui il militare aveva agito e la loro radicale estraneità ai compiti di istituto (procurare informazioni riservate sul conto di un soggetto al coniuge separato del medesimo), ma ha ritenuto abusivo l'accesso in quanto oggettivamente contrastante con la prescrizione di cui si è detto, nonostante lo stesso militare avesse utilizzato le proprie credenziali e le informazioni raccolte rientrassero per tipologia tra quelle per cui egli era legittimato, sussistendone i presupposti, a consultare la banca dati.
In conclusione le Sezioni Unite hanno stabilito 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 pur essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso nel sistema.
3. Orbene, nel caso in esame deve ritenersi assolutamente carente la motivazione della sentenza impugnata in ordine alla sussistenza del delitto di cui all'art. 615 ter cod. pen., tenuto conto del principio di diritto sopra evidenziato.
La Corte territoriale non ha risposto in maniera adeguata e specifica alle doglianze mosse dal ricorrente, che ha sostenuto la legittimità del suo accesso al sistema informatico della società MIDA s.r.l., essendo in possesso delle credenziali in quanto nel periodo contemplato dalla contestazione egli esercitava ancora attività lavorativa per la suddetta società, così come peraltro si desume dalla stessa descrizione dei fatti di cui al capo di imputazione.
Va premesso che il sindacato di questa Corte sulla motivazione del provvedimento impugnato deve essere volto a verificare che quest'ultima:

a) sia "effettiva", ovvero realmente idonea a rappresentare le ragioni che il giudicante ha posto a base della decisione adottata;

b) non sia "manifestamente illogica", perché sorretta, nei suoi punti essenziali, da argomentazioni non viziate da evidenti errori nell'applicazione delle regole della logica;

c) non sia internamente "contraddittoria", ovvero esente da insormontabili incongruenze tra le sue diverse parti o da inconciliabilità logiche tra le affermazioni in essa contenute;

d) non risulti logicamente "incompatibile" con "altri atti del processo" (indicati in termini specifici ed esaustivi dal ricorrente nei motivi posti a sostegno del ricorso) in misura tale da risultarne vanificata o radicalmente inficiata sotto il profilo logico (Sez. 1, n. 41738 del 19/10/2011 - dep. 15/11/2011, Pmt in proc. Longo, Rv. 251516).

Peraltro, va pure precisato che gli atti del processo invocati dal ricorrente a sostegno del dedotto vizio di motivazione non devono semplicemente porsi in contrasto con particolari accertamenti e valutazioni del giudicante, ma devono essere autonomamente dotati di una forza esplicativa o dimostrativa tale che la loro rappresentazione risulti in grado di disarticolare l'intero ragionamento svolto dal giudicante, determinando al suo interno radicali incompatibilità, così da vanificare o da rendere manifestamente incongrua o contraddittoria la motivazione.

Passando, quindi, all'analisi del caso in esame, non avendo rilievo, come si è visto, per la configurazione del reato contestato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso nel sistema, l'affermazione di responsabilità del ricorrente avrebbe dovuto essere specificamente incentrata sulla eventuale violazione delle condizioni e dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso.

Si è allora fatto correttamente riferimento alle regole vigenti nella società MIDA, essendo pacifico che ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico o telematico, la protezione del sistema può essere adottata anche con misure di carattere organizzativo che disciplinino le modalità di accesso, consentito esclusivamente dal titolare per determinate finalità ovvero per il raggiungimento degli scopi aziendali. (Sez. 5, n. 18497 del 18/12/2012 - dep. 24/04/2013, Valenza, Rv. 255924).

La norma del codice adottato dalla società MIDA, richiamata anche dal ricorrente, statuisce quanto segue: "*È fatto assoluto divieto, altresì, di copiare o duplicare files di dati di proprietà di MIDA per finalità che esulano dal trattamento dei dati di propria competenza o dalla semplice copia di backup degli stessi. In nessun caso tali dati potranno essere portati all'esterno della società su qualunque tipo di supporto di memorizzazione, ivi compreso l'invio per posta elettronica ad eccezione di specifiche autorizzazioni del Responsabile EDP*".

Orbene, è evidente che la norma riportata non escluda *tout court* né la copia né la duplicazione dei file; fa divieto, invece, solo di copia o duplicazione "per finalità che esulano dal trattamento dei dati di propria competenza o dalla semplice copia di backup degli stessi", lasciando pertanto lecita la condotta in senso oggettivo.

In effetti, né la Corte territoriale né il giudice di primo grado si sono preoccupati nella loro motivazione di dare giustificazione del percorso logico seguito in primo luogo per dare atto specificamente della condotta di copiatura o duplicazione di file da parte dell'imputato e, soprattutto, della prova che tale condotta non rientrasse nelle finalità del trattamento dei dati di competenza dello stesso G. in quel momento preciso, essendo pacifico che egli all'epoca svolgesse ancora attività lavorativa per la società.

Nella sentenza impugnata, dopo aver riportato la norma del codice sopra trascritta, la Corte territoriale si limita a evidenziare che "*ne segue che la condotta dell'imputato, come sopra accertata, - non importa se attuata all'interno o all'esterno dei locali dell'azienda, ciò essendo irrilevante ai fini della sussistenza del reato- ha indubitabilmente violato le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dalla MIDA s.r.l. per delimitarne oggettivamente l'accesso, sotto un duplice profilo: da un lato l'accesso al server aziendale è stato funzionale alla copiatura di files per finalità che estranee al trattamento dei dati di propria competenza o alla semplice copia di backup; dall'altro i dati copiati sono stati portati all'esterno della società su un supporto di memorizzazione removibile*".

Partendo da tale ultima annotazione della motivazione, va rilevato che non si comprende da quali dati la Corte deduca che le copie dei file, che sarebbero state fatte dal G. , siano state portate all'esterno della società, non essendo stati indicati specificamente gli elementi di prova in base ai quali sono stati delineati i dati temporali e modali di tale condotta. In effetti la Corte ha ritenuto sussistente la circostanza in conseguenza della perdita di clienti da parte della MIDA e dell'acquisizione di tali clienti da parte della società per la quale il G. era andato poi a lavorare. Tale deduzione, però, non è supportata dalla indicazione di elementi di prova riferiti allo specifico fatto che i dati copiati dal G. siano stati poi da questi utilizzati per la sua nuova attività. Peraltro va ribadito che le Sezioni Unite di questa Corte, con la sentenza sopra richiamata, hanno statuito che rilevano, al riguardo, solo quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, mentre sono del tutto irrilevanti, ai fini della configurazione della fattispecie di cui all'art. 615 ter cod. pen., eventuali disposizioni sull'impiego successivo dei dati.

La prima parte, poi, delle suddette considerazioni della Corte territoriale si risolvono in mere asserzioni, non avendo fornito, con argomenti logici e legati specificamente a risultanze probatorie, elementi per ritenere che in effetti la condotta del G. abbia violato le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dalla MIDA s.r.l. ovvero che l'accesso al server aziendale sia stato funzionale alla copiatura di files per "finalità estranee al trattamento dei dati di propria competenza o alla semplice copia di backup".

La Corte d'Appello si limita a richiamare la condotta "come sopra accertata" e nella sentenza, a tal proposito, si legge solo che i fatti erano stati ricostruiti sulla base delle dichiarazioni di un tecnico, consulente incaricato dalla stessa società MIDA, che aveva verificato "la pulizia sistematica dell'hard disk, dal quale erano stati sistematicamente eliminati sia tutti i files, sia la posta elettronica....fatto avvenuto la sera del 29 aprile"; aveva poi verificato che "in data 30 marzo e 6 aprile 2008 una notevole quantità di dati è stata copiata su supporto dvd....Tutte le operazioni furono effettuate con le credenziali personali dell'imputato".

Prosegue la Corte d'Appello con la seguente considerazione conclusiva in punto di fatto: "..i dati inconfutabilmente accertati dal consulente, corroborati dalla disdetta di oltre 100 clienti, confluiti nella società ove G. era andato a lavorare, non lasciano dubbio alcuno che l'imputato, nel mese di aprile 2008, abbia copiato sul computer portatile aziendale che aveva in dotazione, accedendo al server aziendale, una serie di dati sensibili relativi ai clienti della MIDA s.r.l., dati successivamente salvati su un supporto removibile e quindi definitivamente cancellati dall'hard disk del computer portatile prima della restituzione". Si tratta ancora una volta di considerazioni che scaturiscono da un ragionamento deduttivo che trova la sua fonte in circostanze che non possono avere rilievo ai fini della configurabilità del reato contestato, perché fanno riferimento al (peraltro non provato) impiego successivo dei dati che si assumono copiati.
Orbene, tale motivazione non appare supportata da criteri di logicità e coerenza, controllo che compete a questa Corte e che in caso di esito negativo impone l'annullamento per nuovo esame.

Da tempo le Sezioni Unite di questa Corte hanno chiarito che in tema di sindacato del vizio della motivazione, il compito del giudice di legittimità non è quello di sovrapporre la propria valutazione a quella compiuta dai giudici di merito in ordine all'affidabilità delle fonti di prova, bensì di stabilire se questi ultimi abbiano esaminato tutti gli elementi a loro disposizione, se abbiano fornito una corretta interpretazione di essi, dando esaustiva e convincente risposta alle deduzioni delle parti, e se abbiano esattamente applicato le regole della logica nello sviluppo delle argomentazioni che hanno giustificato la scelta di determinate conclusioni a preferenza di altre (Sez. U, n. 930 del 13/12/1995 - dep. 29/01/1996, Clarke, Rv. 203428).

È pur vero che, secondo consolidato orientamento giurisprudenziale, il giudice di merito non ha l'obbligo di soffermarsi a dare conto di ogni singolo elemento indiziario o probatorio acquisito in atti, potendo egli invece limitarsi a porre in luce quelli che, in base al giudizio effettuato, risultano gli elementi essenziali ai fini del decidere, purché tale valutazione risulti logicamente coerente. (Sez. 5, n. 2459 del 17/04/2000 - dep. 08/06/2000, PM in proc. Garasto L, Rv. 216367).

È anche incontroverso, però, che il dovere di motivazione della sentenza è adempiuto, ad opera del giudice del merito, solo attraverso la valutazione globale delle deduzioni delle parti e delle risultanze processuali e devono essere spiegate le ragioni che hanno determinato il convincimento, dimostrando di aver tenuto presente ogni fatto decisivo (Sez. 6, n. 20092 del 04/05/2011 - dep. 20/05/2011, Schowick, Rv. 250105; Sez. 4, n. 1149 del 24/10/2005 - dep. 13/01/2006, Mirabilia, Rv. 233187; Sez. 4, n. 36757 del 04/06/2004 - dep. 17/09/2004, Perino, Rv. 229688).

Come si è evidenziato, nel caso in esame, pur a fronte di doglianze specifiche dell'imputato appellante, la Corte territoriale ha reso una motivazione disarticolata sull'intero ragionamento probatorio e per questo da ritenersi insufficiente ed illogica per la essenziale forza dimostrativa del dato processuale.

4. Anche se l'accoglimento del motivo sopra indicato risulta assorbente rispetto alla valutazione degli altri profili in questione, per completezza va rilevato che egualmente carente ed illogica deve ritenersi la motivazione della sentenza impugnata in ordine alla condanna al risarcimento del danno oltre che al riconoscimento della provvisionale in favore della parte civile.

Fondatamente il ricorrente ha rilevato che i giudici di merito hanno compiuto una deduzione logica palesemente forzata, ritenendo esistente il danno patrimoniale sulla base della sola circostanza che i clienti persi dalla MIDA s.r.l. sarebbero passati rapidamente alla ESEDRA, nuova società nella quale l'imputato era andato a lavorare.
La Corte territoriale, peraltro, non ha tenuto in alcun conto quanto specificamente dedotto dal ricorrente in ordine alla decisione del giudice del lavoro che si è occupato della stessa vicenda e

che ha escluso con sentenza che ci fosse un nesso causale tra la nuova attività lavorativa dell'imputato e il lamentato pregiudizio patrimoniale della MIDA s.r.l., ritenendo che non vi sia alcun collegamento tra l'avvenuta copiatura dei dati aziendali contenenti gli elenchi della clientela e le disdette della stessa clientela.
In ordine alla provvisionale, poi, la motivazione della Corte territoriale è caratterizzata ancora una volta da particolare sintesi assertiva, limitandosi a ritenere che la somma di 30.000 Euro è "sicuramente inferiore ai danni patiti derivanti sia dalla disdetta dei mandati di brokeraggio assicurativo, sia dalla distruzione dei files contenenti fondamentali informazioni sui clienti".

4. Sulla base delle suesposte considerazioni, l'impugnata sentenza deve essere annullata con rinvio per nuovo giudizio ad altra Sezione della Corte d'appello di Milano, che nella piena libertà delle valutazioni di merito di sua competenza dovrà porre rimedio alle rilevate carenze motivazionali, uniformandosi al quadro dei principi di diritto in questa sede stabiliti.

P.Q.M.

La Corte annulla la sentenza impugnata con rinvio ad altra sezione della Corte di Appello di Milano per nuovo esame.