Motivi della decisione

D. M, P. V. e P. I. L. sono stati rinviati a giudizio per rispondere del reato di cui agli artt. 110-615 ter comm1 e 2 n. 3 c.p. per essersi abusivamente introdotti nel sistema informatico aziendale della N U s.r.l., per aver acquisito tutti i dati ivi contenuti ed aver cancellato la registrazione sul sistema aziendale. Il 20.6.07.

Il decreto è stato in particolare emesso a seguito di annullamento della sentenza di non luogo a procedere emessa ex art. 425 c.p.p. dal Gup da parte della Corte di Cassazione (investita del ricorso promosso dalla parte civile).

Gli imputati sono comparsi ed hanno partecipato al processo.

N.U srl, già costituitasi parte civile nel corso dell'udienza preliminare, ha poi revocato detta costituzione all'udienza del 13.12.10.

In sede istruttoria sono stati sentiti i testi W. P., consulente informatico cui è stato affidato nell'immediatezza dei fatti un accertamento informatico da parte dei vertici della citata società, A.M e C. V., all'epoca dei fatti rispettivamente legale rappresentante e socio della stessa società, indicati quali testi da tutte le parti (ad eccezione di V indicato dalle sole difese).

Le parti hanno inoltre prodotto documentazione ed in particolare lettera di licenziamento di N.U. nei confronti di D. M e P. V. a seguito dei fatti di causa ed atti relativi alla causa di lavoro avviata a seguito di ricorso avverso il licenziamento promosso dai due dipendenti con relative sentenze passate in giudicato. Con il consenso delle parti il P.m. ha prodotto i verbali degli interrogatori resi dagli imputati nel corso delle indagini.

Ad esito dell'istruttoria è stata rigettata la richiesta avanzata dalle difese in sede di ammissione prove di acquisizione dell' hard disk contenente il back up eseguito da P. V. il giorno dei fatti sul p.c. che aveva in uso per lavoro presso la citata N.U: nonché di perizia sullo stesso.

Ad esito del dibattimento le parti hanno chiesto tutte l'assoluzione degli imputati perché il fatto non sussiste ed è stata pronunciata sentenza di assoluzione in accoglimento delle istanze delle parti per i motivi qui di seguito riportati.

La vicenda ha preso le mosse dalla querela presentata il 25.6.07 da A.M, in qualità di legale rappresentante di N.U:, nei confronti di tutti e tre gli imputati per furto dei dati informatici contenuti nel p.c. aziendale e danneggiamento, stante l'avvenuta cancellazione dei dati trafugati dal server centrale. A tale querela seguiva un'integrazione nei confronti dei soli V. e M, datata 28.11.07, con la quale si lamentava il furto di alcuni beni materiali.

Da tale querela scaturiva il presente procedimento (nel quale originariamente era contestato agli imputati M e V anche il furto di beni materiali appartenenti a N.U:) nell'ambito del quale il Gup il 13.1.09 pronunciava sentenza ex art. 425 c.p.p.
In particolare il Gup (premessa in fatto la prova dell'accesso da parte di P. V. ai dati informatici aziendali e della copiatura di alcuni di essi su un hard disk esterno ed esclusa quella dell'avvenuta distruzione dell'archivio informatico aziendale anche a mezzo mera copiatura dal momento che detta copiatura aveva riguardato esclusivamente i dati presenti sul p.c. in uso a P. V. e non anche il back up dei medesimi presente sull'hard disk centrale), ha escluso l'abusività dell'accesso sul presupposto in diritto che non integra il reato l'accesso effettuato da chi vi abbia titolo quand'anche la finalità del medesimo sia illecita (dovendosi il tal caso rispondere esclusivamente dei reati diversi che risultino eventualmente configurabili).

Avverso detta sentenza, seppur con riguardo esclusivo all'imputazione di cui all'art. 615 ter c.p., la parte civile promuoveva ricorso per Cassazione e la Corte di Cassazione con sentenza del 10.12.09 annullava la sentenza affermando il seguente principio: integra il reato di accesso abusivo ad un sistema informatico o

telematico la condotta del soggetto che, pur avendo titolo per accedere al sistema, vi si introduca con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico.

Con riguardo alla questione giuridica affrontata nelle due sentenze testé citate è opportuno sottolineare fin d'ora e prima di analizzare il merito che le stesse sono espressione dei due indirizzi sviluppatisi nella giurisprudenza della Corte di Cassazione, medio tempore tuttavia superati dalla sentenza n. 4694 del 2012 delle Sezioni Unite. Con detta sentenza la Corte ha statuito l'irrilevanza 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 e 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 determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta" .

Tanto premesso si ritiene che, alla luce di quanto si dirà in ordine agli elementi di fatto presenti in atti, il menzionato indirizzo giurisprudenziale delle sezioni unite, assuma rilevanza nel presente procedimento e porti ad escludere la sussistenza del reato sotto il profilo della illegittimità dell'accesso posto che si ritiene sia provato in atti l'accesso da parte di P. V., in concorso con gli altri due imputati, nel sistema informatico protetto da sistemi di sicurezza di N.U:, e che tuttavia lo stesso sia avvenuto nell'ambito dell'autorizzazione (e dei limiti della stessa) rilasciata alla V da parte dell'azienda (a prescindere dalle finalità lecite o meno dello stesso).

Deve peraltro aggiungersi che non essendosi raggiunta pienamente la prova della illiceità e/o della estraneità rispetto agli scopi sottostanti alla protezione dell'archivio informatico delle finalità perseguite dall'agente, una sentenza assolutoria si impone anche sulla base del principio affermato dalla Corte di Cassazione nel presente procedimento.

Si ritiene che del citato mutamento di indirizzo giurisprudenziale debba tenere conto questo giudice nell'ambito di una interpretazione dell'art. 627 comma 3 c.p.p. conforme al diritto Cedu, in particolare art. 7, come interpretato dalla Corte Edu.
Di tale necessità si è fatta interprete in altro ambito (in materia di esecuzione) la stessa Corte di Cassazione a sezioni unite chiamata a decidere se il mutamento di giurisprudenza intervenuto medio tempore con decisione delle sezioni unite renda ammissibile la riproposizione della richiesta di applicazione dell'indulto in precedenza rigettata. Ebbene la Corte ha risposto positivamente al quesito affermando che l'obbligo di interpretazione conforme alla Cedu impone di includere nel concetto di nuovo elemento di diritto idoneo a superare la preclusione di cui al secondo comma dell'art. 666 c.p.p. anche il mutamento giurisprudenziale che assume, specie in conseguenza di un intervento del supremo organo di nomofilachia, il carattere della stabilità ed integra il diritto vivente unite (sentenza n. 18288/10 Beschi).
Mutatis mutandis, e ritenuto che l'obbligo del giudice del rinvio di uniformarsi ai principi di diritto sanciti dalla Corte di Cassazione di cui al richiamato art. 627 comma 3 c.p. sia superato da un "nuovo elemento di diritto" (si tratta della dizione riportata nell'art. 666 c.p.p.) che faccia venir meno la rilevanza penale della condotta tenuta dall'agente in ossequio ai principi di rango costituzionale di cui all'art. 25 Cost. ripresi dall'art. 2 c.p., deve concludersi che il principio affermato dalle sezioni unite con la sentenza 4694/12, in quanto favorevole all'imputato e volto a tutelare i diritti fondamentali espressi nel caso di specie dall'art. 25 Cost., debba essere osservato (peraltro lo stesso potrebbe validamente fondare un incidente di esecuzione avverso la presente sentenza ex art. 666 c.p.p. citato) .

Quanto all'argomento contrario che si fonda sull'intangibilità del giudicato, si richiamano non solo i limiti all'inderogabilità dello stesso sanciti dal nostro ordinamento, che, come noto, disciplina il contrasto di giudicati ma, ancora, la giurisprudenza della Cedu recepita dalla Corte Costituzionale (v. sent 317 del 2009 sul processo in absentia).

Passando ora al merito, è pacifico (ciò risulta anche dalla ricostruzione dei fatti offerta dalla teste A M) che al momento dei fatti i coniugi D. M (quest'ultimo era anche socio al 30% insieme alla sorella A -40%- ed a C. V. -30%-) e P. V. erano dipendenti della più volte citata società impegnata nel settore degli allestimenti per stand fieristici.

P. V. in particolare era addetta ai rapporti con i clienti e con i fornitori.

E' del pari pacifico che la società disponeva di un sistema informatico protetto da misure di sicurezza. Tale è invero pacificamente la predisposizione di un sistema di password predisposto per interdire l'accesso a chi non fosse dotato delle stesse. In tale contesto aziendale P. V. aveva una sua postazione informatica e godeva di una password che le consentiva l'accesso ai dati informatici della società. La stessa tuttavia non aveva accesso, e la password nella sua disponibilità non lo consentiva, all'hard disk centrale nel quale confluivano, grazie ad un sistema in parte automatizzato di back up, i dati presenti sui p.c. personali).

Il 20 giugno 2007 verso le 18.00 P. V. è certamente entrata nel proprio ufficio presso la sede di Ar ove prestava abitualmente la propria attività in compagnia dell'amica P L ed il giorno successivo è stata accusata di aver in detta occasione copiato dal proprio p.c. tutti i files presenti, quali progetti relativi agli stand, ordini clienti già evasi o da evadere con cancellazione dei medesimi anche dall'hard disk centrale.

L'imputata ha ammesso di aver, con l'aiuto della L, e nella citata occasione, cancellato dalla memoria del proprio p.c. alcuni files personali quali fotografie, referti medici e mail personali, di aver copiato, esclusivamente dal proprio p.c., i dati presenti relativi al lavoro da lei svolto in relazione a clienti e fornitori e di non aver quindi in alcun modo cancellato i dati presenti sul server centrale sul quale quotidianamente veniva fatto il back up dei dati presenti sui tre p.c. aziendali e pertanto necessariamente dovevano trovarsi anche i dati copiati e cancellati dal proprio p.c. (cfr interrogatorio e dichiarazioni rese nell'ambito del processo davanti al giudice del lavoro avente ad oggetto il licenziamento della stessa V nonché interrogatorio reso dagli altri due imputati)

Questa ricostruzione dei fatti ha trovato conferma nell'accertamento tecnico che gli stessi vertici di N.U: hanno nell'immediatezza affidato a W. P.. Costui sentito come teste ha in particolare escluso, richiamando la relazione scritta redatta allorchè ha svolto l'indagine, di poter concludere che nell'occasione considerata siano stati cancellati dati dal server centrale (il tecnico così si è espresso: "io ho potuto constatare che è stato installato il software di sincronizzazione: questo attesta l'avvenuta sincronizzazione ma non si può verificare l'effettiva importazione o esportazione dei dati. Potrebbe essere stata una semplice sincronizzazione di una rubrica di cellulare verso la rubrica di out look. La cancellazione della posta informatica che abbiamo potuto riscontrare non è necessariamente riconducibile alla data dell'ultimo accesso anzi certamente si tratta di cancellazioni avvenute nell'arco del tempo; non è possibile distinguere quanto è stato cancellato man mano da quello che eventualmente è stato cancellato con l'ultimo accesso. Abbiamo recuperato sia le mail cancellate sia i file cancellati dal pc p. La maggior parte di cancellazione di mail afferisce al periodo gennaio aprile 2007.").

Sul punto, considerato che come riferito dal teste P la cancellazione abbia riguardato legittimamente e nel corso dei mesi files che non era utile o necessario conservare (si pensi alle mail che ognuno di noi quotidianamente cancella), rilevante appare la circostanza che i vertici di N.U: non abbiano mai indicato specificamente i files asseritamente mancanti.

Tale accertamento ha costituito il fondamento della richiesta di assoluzione avanzata dal p.m. e dalla difesa.

Ritiene questo giudice che detta evidenza escluda esclusivamente la sussistenza dell'ipotesi delittuosa contestata di cui al comma 2 n. 3 dell'art. 615 ter c.p. ma non anche, astrattamente, quella meno grave di cui

al comma 1 della stessa norma che punisce il mero accesso illegittimo in un sistema informatico e/o telematico protetto da misure di sicurezza.

Sotto questo profilo assumono rilevanza i principi espressi dalla Corte di Cassazione sopra richiamati.

Come più sopra anticipato (la circostanza è riferita in termini generali anche da A M) P. V. aveva il pieno e incondizionato accesso ai dati cui ha fatto accesso nell'occasione considerata. Si trattava di dati relativi a clienti e fornitori, di ordini, di progetti relativi ai medesimi che costituivano i quotidiani strumenti di lavoro della dipendente e che la stessa aveva avuto sin ad allora anche la facoltà di copiare. L'accesso agli stessi come detto era incondizionato e pertanto, alla luce dei principi espressi dalle sezioni unite con la sentenza richiamata più sopra, l'accesso e la permanenza nel sistema da parte della V dovevano ritenersi legittimi. Un esempio valga a chiarire il punto. Nel caso sottoposto al vaglio della Corte di Cassazione citata, l'accesso era stato effettuato da un appartenente alle forze dell'ordine ed aveva riguardato la banca dati interforze contenente tra l'altro i precedenti penali e di polizia dei soggetti schedati. Nel caso di specie l'accesso era stato ritenuto illegittimo perché l'utente, pur in possesso di password legittimante l'ingresso nel sistema, ciò aveva fatto al di fuori dei limiti posti a tale accesso ed in particolare in assenza dei presupposti del medesimo, quali in particolare l'esistenza di un procedimento amministrativo o penale nei confronti del soggetto cui i dati afferivano o nel quale il medesimo fosse ad altro titolo coinvolto.

Infine, per completezza, si rileva che il dibattimento non ha provato oltre ogni ragionevole dubbio che la finalità dell'accesso fosse illecita e/o estranea agli scopi sottostanti alla protezione dell'archivio, circostanza rilevante secondo il principio espresso dalla Corte di Cassazione che ha annullato la sentenza del Gip nell'ambito del presente procedimento.

Invero, secondo la versione resa dagli imputati e solo genericamente smentita da A M, in occasione di una riunione tenutasi qualche giorno prima dei fatti, stanti gli attriti tra A M e P. V. e la volontà della prima di licenziare la seconda, nonché, sotto altro profilo, le tensioni tra la stessa A ed il compagno di costei (quest'ultimo era anche il finanziatore dell'intera operazione commerciale, P S) si era deciso di liquidare la società e la relativa procedura era stata affidata al commercialista, dott A. Per tale ragione P. V. aveva in particolare ritenuto che fosse legittimo copiare quello che riteneva fosse il frutto del suo lavoro, ed in particolare i contatti con clienti e fornitori, senza peraltro sottrarlo ad altri.

Tale ricostruzione che, come detto, non trova smentita definitiva in altre fonti di prova (le testimonianze di A M e di C. V. sul punto, peraltro, come detto generiche, non appaiono risolutive stante il clima conflittuale presente in azienda al momento dei fatti) non consente di ritenere provato che l'asportazione dei dati dal p.c. personale fosse illecita e, come espressamente sancito dalla Corte, soprattutto, estranea agli scopi sottostanti alla protezione dell'archivio informatico.
In subordine, non vi è prova che della eventuale illiceità e/o lesività del bene protetto fossero consapevoli P. V., D. M e, *a fortiori*, P L. A sostegno di tale ultimo punto si rammenta peraltro che, come accertato in sede di giudizio lavoristico, nei giorni immediatamente successivi alla contestazione mossagli dalla datrice di lavoro, P. V. aveva messo a disposizione dell'azienda i dati copiati.

p.q.m.

visto l'art. 530 c.p.p.

assolve

D. M, P. V. e P. I. L. dal reato ai medesimi contestato perché il fatto non sussiste.
Motivazione in giorni 60.
Milano, 11 maggio 2012

Il Giudice