TRIBUNALE DI MODENA
SEZ. PENALE

Ordinanza 28 settembre 2016

Il Tribunale,

a scioglimento della riserva assunta all'udienza del 26.09.2016 sulle eccezioni verbalizzate in quella sede,

osserva quanto segue.

Nella nostra legislazione penale sostanziale il concetto di documento informatico si è affermato progressivamente. Infatti, con la L. 23 dicembre 1993, n.547, ("*Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*"), sono state apportate significative modifiche ad alcune fattispecie incriminatrici e ne sono state introdotte di nuove, tendenti ad estendere la tutela penale, non solo ai sistemi e alle apparecchiature informatiche e telematiche, ma anche ai loro "prodotti", vale a dire ai documenti elaborati con tali sistemi, presenti in essi e trasmessi attraverso di essi.

Ma il documento aveva ancora una consistenza corporale in quanto il legislatore, evidentemente, riteneva di non poter tutelare il contenuto, senza tutelare il contenitore, vale a dire, appunto, il supporto materiale (floppy, pen-drive, hard disk, nastro magnetico ecc.) che incorpora il documento.

Successivamente, però, la L. 18 marzo 2008, n.48, esecutiva della convenzione di Budapest (Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2011), ha mutato prospettiva ed affermato che il documento informatico non si identifica più - come una volta - con il suo supporto, ma col dato in esso contenuto. Si tratta dunque di un documento immateriale, che non si incorpora in un oggetto fisico (così come il pensiero non si incorpora nell'apparato cerebrale che lo produce e lo "immagazzina").

Il successivo "passo" (compiuto appunto con la legge 48/2008) è consistito nel ritenere il documento informatico, non una copia, una riproduzione, una trasposizione virtuale di un documento materiale, ma un documento in sé.

Lo scopo della equiparazione è evidente: assicurare la certezza e la affidabilità dei dati informatici relativi ai rapporti giuridici.

Con tale impostazione, poi, è stato coerente il coevo sviluppo della legislazione penalistica in tema di reati informatici: così è stata introdotta l'ipotesi *ex* art. 495 *bis* c.p. ("*Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri*"), che mira a tutelare

la genuinità delle dichiarazioni destinate ad essere inserite in un documento elettronico. E ancora può essere ricordato l'art. 615 *quater* c.p., che proibisce e punisce la detenzione e diffusione di codici di accesso (ovviamente immateriali, trattandosi di semplici sequenze alfanumeriche) a sistemi informatici e telematici, ma anche l'art. 617 *sexies* c.p., che reprime la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche e così via.

È un dato ormai assodato che, tanto nei rapporti interpersonali, quanto nella sfera giuridica, il processo di smaterializzazione del documento è in atto e progredisce rapidamente. La stessa giurisprudenza penale di legittimità se ne è ben resa conto, atteso che, ad es., ha ritenuto sussistenti le ipotesi di falsità in certificazioni con riferimento ai dati contenuti in archivi informatici, ed ha addirittura ravvisato, facendo logica applicazione del "nuovo" concetto di documento, il delitto di bancarotta semplice documentale nel caso di perdita, per comportamento negligente o imprudente, della memoria informatica del computer, contenente le annotazioni delle indicazioni contabili (ASN 200935886- RV 244921).

Ora è indubbio che, se il Legislatore ha inteso tutelare addirittura con la sanzione penale il "documento informatico", ne ha certamente presupposto non solo l'esistenza, ma la sua "cittadinanza" nell'intero universo giuridico. La sanzione penale, infatti, è meramente funzionale alla tutela di un bene/interesse dato per preesistente, un bene/interesse che certamente essa non crea, ma si limita a proteggere.

Ebbene, applicando tali principi nel campo processuale, deve porsi l'attenzione - per quello che qui interessa - sulle modalità di acquisizione degli elementi di prova processualmente utilizzabili.

Si pone, invero, un duplice ordine di problemi: quello relativo alla individuazione degli strumenti giuridici più opportuni che la procedura penale mette a disposizione per la ricerca della prova e quello relativo alle modalità tecniche di acquisizione, trattamento e custodia delle prove che risiedono in memorie di massa.

Il tutto tenendo conto dei diritti e delle garanzie dell'indagato.

Ed allora non è un caso che la legge n.58 del 2008 abbia introdotto il comma 1-*bis* all'art. 247 c.p.p. che testualmente recita '*quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*'.

In stretta conseguenzialità con la norma appena citata l'art. 254 *bis* c.p.p. - sempre introdotto dalla novella del 2008 - prevede che '*l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di*

telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico e di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità'.

Ma spesso, in luogo del sequestro, il PM può orientare l'acquisizione di elementi di prova attraverso l'ispezione con un minor impatto sull'ordinaria attività del soggetto (che nel caso in esame quando il PC è utilizzato anche per motivi di lavoro o trattasi di apparati informatici di aziende di grandi dimensioni), mediante l'effettuazione sul posto di una copia delle memorie digitali da parte di un esperto in veste di ausiliario di PG e compatibilmente con la situazione logistica e temporale contingente. Ed in tale ottica la novella del 2008 ha modificato anche l'art. 244 c.p.p. in tema di ispezioni, prevedendo che l'autorità giudiziaria può disporre ogni altra operazione tecnica '*anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*'.

L'attenzione che il legislatore riserva alle tecniche di cd *computer forensic* per la ricerca di evidenze digitali è finalizzata a far sì che durante tutto l'arco del procedimento penale il Pm possa essere in grado di dimostrare che la copia in suo possesso sia perfettamente identica a quella in possesso dell'indagato o del terzo non sottoposto ad indagini ma in possesso del materiale probatorio al momento dell'intervento.

Tirando le fila del discorso sin qui fatto deve registrarsi una sostanziale equipollenza del mezzo di ricerca della prova utilizzato (ispezione, perquisizione e sequestro) ma un evidente *favor* verso modalità di acquisizione che documentino l'assoluta identità tra dati originali e dati copiati.

Tali conclusioni attengono ai casi in cui l'oggetto materiale dell'attività di acquisizione sia rappresentato da '*dati, informazioni, programmi informatici o tracce pertinenti al reato*' (nozione contenuta nell'art. 247 comma 1*bis* c.p.p. e più ampia di quella contenuta nell'art. 254 *bis* c.p.p.).

Nel caso in esame, l'attività di acquisizione - peraltro attuata con la richiesta al gestore *ex* art. 132 D.Lvo 196/03 - non ha riguardato solo i dati esterni relative alle comunicazioni di posta elettronica, ma il contenuto delle medesime.

Sul punto va ricordato che la posta elettronica (cd e-mail) consiste nel mandare messaggi attraverso la rete: i destinatari del messaggio li riceveranno sul PC non appena attivata la connessione.

Presupposto, pertanto, per la fruizione del servizio di posta elettronica è il possesso da parte dell'utente di un 'indirizzo e-mail' cui è direttamente collegato il possesso di una casella postale sempre presente e ricettiva, solitamente localizzata in appositi sistemi presso *Internet Service Provider*.

Già nel 1999, con pronuncia n.23 del 12 luglio, l'Autorità Garante per la protezione dei dati personali aveva stabilito che i messaggi di posta elettronica devono essere considerati come corrispondenza privata ed in quanto tali non possono essere violati e non possono essere abusivamente intercettati.

Invero, l'accesso ad una casella di posta elettronica è normalmente soggetta ad una autenticazione mediante l'inserimento della password, la modalità di accesso al servizio è inoltre asincrona in quanto non è necessario che mittente e destinatario siano contemporaneamente attivi o collegati.

Ed allora, sarà possibile il sequestro di corrispondenza telematica allocata nel PC del soggetto indagato o giacente presso i gestori con le forme stabilite dall'art. 254 e 254 *bis* c.p.p. e alle condizioni stabilite dall'art. 247 comma 1 *bis* c.p.p..

Nel caso in esame, invece, il PM ha sostanzialmente equiparato tale attività al trattamento previsto per l'acquisizione dei cd tabulati telefonici contenenti i dati esterni identificativi delle comunicazioni telefoniche e conservati in archivi informatici del gestore del servizio. Invero, per acquisire tali dati, da tempo, le SSUU (23.2.2000) hanno affermato che è sufficiente il decreto motivato dell'autorità giudiziaria non essendo necessaria, per il minore grado d'intrusione nella sfera di riservatezza, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni stabilite dall'art. 266 e ss c.p.p..

E a tale determinazione l'organo inquirente è giunto attraverso la svalutazione dei files '*inerenti attività comunicativa in dati decodificati ed allocati nel PC, sfasati cronologicamente con il momento dello scambio comunicativo al fine di considerarli meri documenti presenti nella memoria del PC o del gestore*'.

Tale equiparazione, a parere del Tribunale, non è ammissibile in quanto l'art. 132 del D.Lvo 196/2003 quando si occupa dei dati relativi al traffico telematico esclude espressamente i contenuti delle comunicazioni. Inoltre, stabilisce un limite temporale a ritroso di dodici mesi antecedenti la comunicazione: per le e-mail anteriori al [OMISSIS] i dati comunque acquisiti sono patologicamente inutilizzabili (così Cass. 5.12.2014 n.15613 e di recente Cass. pen. sez. V, 25/01/2016, n.7265).

Ma il dato processualmente più significativo è quello relativo al rispetto delle garanzie difensive che in materia di corrispondenza privata avrebbe dovuto imporre l'adozione del provvedimento di sequestro con obbligo di avvertire l'indagato e facoltà per il medesimo di farsi assistere da un legale e - in relazione alle operazioni di estrazione di copia dal PC o dai server del gestore informatico - di svolgere in contraddittorio le attività tecniche con sistemi che garantissero la maggiore affidabilità possibile della copia estratta dalla memoria della posta elettronica.

Invero, dal punto di vista delle modalità acquisitive, si è in presenza di una evidente carenza di quegli accorgimenti tecnici richiamati nelle norme sopra esaminate e introdotti dalla legge n.48 del 2008 anche se sul punto, la giurisprudenza ha chiarito (Cass. 1.7.2015) che '*la mancata adozione di tali modalità* [accertamenti tecnici irripetibili, n.d.e.] *non comporta l'inutilizzabilità dei risultati probatori acquisiti, ma la necessità di valutare, in concreto, la sussistenza di alterazione dei dati originali e la corrispondenza ad essi di quelli estratti*'.

Il Tribunale ritiene in conclusione come ci si trovi in presenza di una attività di intrusione investigativa sulla corrispondenza privata che, rispetto alla normativa generale in tema di sequestri, si atteggia quale disciplina speciale in quanto incidente su aspetti presidiati dall'art. 15 Cost nonché dall'art. 8 CEDU.

Ci si trova al cospetto di un area presidiata dall'art. 15 della carta costituzionale con operatività della riserva di legge e di giurisdizione. Le modalità operative attuate dal PM hanno eluso tale riserva violando la segretezza della corrispondenza.

Per tale motivo, restano viziati da patologica inutilizzabilità tutti i dati di posta elettronica acquisiti in violazione del limite temporale di 12 mesi stabilito dall'art. 132 D.Lvo 196/03 e relativo a quelli antecedenti al [OMISSIS].

Vanno, altresì, dichiarati inutilizzabili tutte le comunicazioni private contenute nelle mail estratte nel tempo di 12 mesi antecedente alla richiesta avanzata dal PM: si verte, in tal caso, in ipotesi di inutilizzabilità (e non di nullità, per la quale potrebbe evocarsi la regola della tassatività delle relative ipotesi), che è la sanzione che scatta in presenza di un atto assunto in violazione di un divieto probatorio, posto a tutela dei diritti fondamentali della persona (quale il diritto alla inviolabilità del domicilio o della corrispondenza).

L'atto investigativo adottato dal PM e il suo prodotto probatorio presentano una residua area di utilizzabilità da circoscrivere ai soli dati esterni relativi a mittente, destinatario o ricevente, nonché ora e giorno ed anno di trasmissione: sul punto, dopo la restituzione dei CD e DVD al PM, sarà cura dell'organo inquirente - se ritenuto necessario a fini di prova - estrapolare un elenco al netto delle dichiarazioni di inutilizzabilità sopra indicate.

In relazione al captatore informatico che il PM ha inserito nel PC della [OMISSIS] e alle risultanze di tale attività intrusiva compendiate nel CD di cui si chiede la acquisizione, il Tribunale non può non rilevare come su tale complessa attività tecnica attuata sul PC di persona indagata sia intervenuta di recente la Suprema Corte di Cassazione a SSUU con sentenza del 28 aprile 2016 che affrontando la questione "*se - anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa - sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone ecc.)*" ha

affermato che ciò è possibile "*limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica (a norma dell'art. 13 d.l. n.152 del 1991), intendendosi per tali quelli elencati nell'art. 51, commi 3-bis e 3-quater, cod. proc. pen., nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato*".

Nel presente procedimento le contestazioni non solo sono estranee alle ipotesi previste dall'art. 51 commi 3 *bis* e 3 *quater* c.p.p., ma soprattutto non vi è stato alcun ricorso al controllo giurisdizionale di cui agli art. 266 e ss c.p.p. relativo alla disciplina sulle intercettazioni.

Nella esecuzione della sua attività captativa, il PM ha ritenuto di dover aderire a quella risalente giurisprudenza secondo cui "*è legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati.* (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico" ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)" (Cass. pen. sez. V, 14/10/2009, n.16556) ma ciò era possibile a condizione che il dato acquisito non avesse ad oggetto un flusso di comunicazioni, come, invece avviene nel caso di controllo delle attività svolte dal PC, con conseguente necessità di attivare i meccanismi di garanzia previsti per lo svolgimento di attività di intercettazione.

Anche il dato probatorio acquisito con le modalità sopra evidenziate resta colpito dalla sanzione di inutilizzabilità e si va ad iscrivere nell'area presidiata dall'art. 191 c.p.p..

P.Q.M.

Visto l'art. 191 c.p.p.,

in accoglimento delle eccezioni proposte dalle difese dichiara la inutilizzabilità del contenuto del CD e DVD estrapolati a seguito di controllo a distanza del personal computer in uso [OMISSIS]; dichiara l'inutilizzabilità nei limiti indicati in parte motiva dei restanti 2 CD e 2 DVD ed ordina la restituzione del materiale al Pubblico Ministero.

Modena, 28.09.2016

Il Presidente