Email aperta - Email chiusa: un problema tutt'altro che risolto

Date : 30 gennaio 2018

Ricordo ancora un caro amico che forte del brocardo latino “Verba volant, scripta manent” mi raccontava che tutte le comunicazioni professionali che lui faceva dovevano necessariamente avvenire tramite fax, in quanto quello strumento gli assicurava da un lato prova dell’invio del documento e dall’altro che ciò che aveva voluto comunicare all’interlocutore rimaneva scritto ed indelebile nel tempo.

Non entrerò nel merito su quanto sosteneva questo amico (anche perché, ricordo che sulla carta chimica usata all’epoca, di indelebile rimaneva ben poco!), ma prendo lo spunto da questo ricordo per evidenziare come oggi, scomparsi i fax, sostituiti dalle email, quel mio amico avrebbe sostenuto che le comunicazioni professionali devono avvenire via email!

Ormai tutti comunicano attraverso email. Invero molti dei servizi tra pubblica amministrazione e privati ormai richiedono necessariamente una email, quasi sempre “certificata” (PEC) e ormai l’email è entrata a far parte dei cosiddetti “campi obbligatori” della modulistica che dobbiamo compilare per iscrizioni, servizi, etc. Potremo ormai dire che la email come il nome il cognome, la data di nascita, il codice fiscale, il numero di telefono e l’indirizzo civico, fa parte delle nostre “generalità”.

Per farla breve, le email oggi rappresentano un diffuso, efficace, comodo e rapido mezzo di comunicazione. Tralascio l’aspetto “riservato” ricordando che già nel 2013 il “Fatto Quotidiano” pubblicò un articolo nel quale evidenziava che i legali di GOOGLE sostenevano in una risposta fornita nell’ambito di una “Class Action” che chi mandava messaggi di posta elettronica via Gmail non aveva alcuna garanzia di riservatezza[1].

Ad ogni buon conto, le email oggi costituiscono un utilizzatissimo mezzo di comunicazione, ne è riprova l’alto interesse che rappresentano in tutti gli ambiti investigativi: civili, penali e amministrativi, atteso che ormai, non esiste indagine che direttamente o indirettamente non prenda in considerazione le comunicazioni email avvenute tra due o più interlocutori, sia allorquando la stessa email possa essere considerata “prova” diretta, sia allorquando la stessa costituisca elemento indiziario a sostegno di una tesi investigativa, basata su altri elementi di prova.

Prima di proseguire, però, vorrei riepilogare in sintesi il quadro normativo vigente circa la "natura" delle comunicazioni email.

L'art. 15 della Costituzione stabilisce che:

"La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

E qui occorre rilevare la lungimiranza dell'Assemblea Costituente che con quel "*ogni altra forma di comunicazione" (*cd. "clausola aperta") permetteva al "futuro" legislatore di adattare la Costituzione all'evoluzione tecnologica che ne sarebbe seguita. Ne da "testimonianza" l'intervento legislativo operato con l'art. 5, L. 23 dicembre 1993, n. 547, che ha modificato l'ultima parte dell'art. 616 del codice penale (Violazione, sottrazione e soppressione di corrispondenza):

"Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.

Il delitto è punibile a querela della persona offesa.

Agli effetti delle disposizioni di questa sezione, per corrispondenza s'intende quella epistolare, telegrafica o telefonica, ***informatica o telematica*** *ovvero effettuata con ogni altra forma di comunicazione a distanza".*

Nonostante gli sforzi dell'Assemblea Costituente e del legislatore, tuttavia, ancora oggi vi è un acceso dibattito tra dottrina e giurisprudenza in relazione a concetti fondamentali per l'interprete quali quelli di e-mail "aperta" ed e-mail "chiusa", proprio con riferimento all'art. 616 del codice penale testé citato, che anche da tale differenza fa dipendere la sussistenza o meno del reato.

Inutile qui richiamare, anche perché non oggetto di questa mia dissertazione, le diverse e non sempre concordi Sentenze che di volta in volta hanno esaminato e sono intervenute su questi due aspetti nel tentativo, spesso infruttuoso, se non impossibile, di assimilare in tutto e per tutto le caratteristiche della corrispondenza cartacea a quelle delle corrispondenza elettronica, ovvero di assimilare una "corrispondenza" avente caratteristiche fisiche ben determinate (un foglio di carta, un tratto grafico, una busta sempre di carta chiusa sui lembi) ad una

corrispondenza definita elettronica, volatile ed immateriale, se non altro, per buona parte della sua esistenza.

Alcuni autori, tendono in merito ai concetti di "e-mail aperta/e-mail chiusa"[2] ad evidenziare tre posizioni dottrinali: una restrittiva che vede nel divieto di analogia, la conseguente ed ovvia considerazione di email sempre aperta non potendosi qualificare la corrispondenza telematica, quale corrispondenza cartacea; una "estensiva" che al contrario considera le email corrispondenza, sempre chiusa; ed una intermedia apprezzata anche dagli autori già citati in nota a piè di pagina, che considera il messaggio email sempre aperto, salvo siano stati utilizzate tecnologie di crittografia a tutela del contenuto.

Occorre comunque rilevare, come il panorama testé esposto, non aiuti l'operatore di polizia allorquando si trovi di fronte alla problematica di dover procedere all'acquisizione di email, soprattutto quando alle predette problematiche più squisitamente "processuali" si aggiungono anche difficoltà di natura tecnica e, mi sia concesso, anche pratiche legate all'acquisizione delle "posta elettronica".

Tra queste difficoltà tecnico pratiche cito, a mero titolo di esempio e lungi dall'essere esaustivo,: l'acquisizione delle "webmail", le difficoltà di acquisizione di un messaggio "bit stream-image", i tempi non sempre a disposizione ma necessari per l'analisi di archivi di posta di diversi Gigabyte, l'effettuazione di operazioni cosiddette "salto nel vuoto" allorquando si lanciano software di acquisizione delle email quali MailStore[3] o Google Takeout[4] che al di là degli innumerevoli pregi di semplicità ed affidabilità hanno il difetto di non fornire una stima del tempo necessario all'effettuazione delle operazioni (cosa non di poco conto per chi effettua operazioni di polizia spesso a carattere coercitivo). Ed ancora mi piace ricordare:

- tutte quelle problematiche di "sincronizzazione" delle email che spesso si risolvono nel ricaricare all'infinito e più volte un medesimo archivio di una webmail su Outlook (mi perdonino gli utilizzatori di "Office"), con il risultato che accade sovente che mail già scaricate e lette vengano riscaricate "come NON lette";
- Tutte quelle difficoltà "tecniche" legate all'utilizzo di alcuni client di posta, o meglio a suite complete quali Lotus Notes, che complicano ulteriormente quelle elementari operazioni di esportazione delle email in formati poi leggibili anche attraverso altri client.

Qui però vorrei trattare nello specifico della cosiddetta "posta elettronica aziendale" ovvero quelle mail aventi dominio @nomeazienda ed assegnate quasi sempre a ciascun soggetto dipendente, identificato attraverso il proprio nome e cognome.

Una delle sentenze che ha cercato di affrontare "di petto" il tema email aperta/email chiusa è stata la sentenza CASSAZIONE PENALE, Sez. V, 19 dicembre 2007, n. 47096. Qui la Suprema Corte della Cassazione prendeva posizione circa la legittimità della condotta di un titolare/superiore gerarchico che aveva preso cognizione del contenuto della corrispondenza di posta elettronica aziendale di un proprio dipendente.

La legittimità dell'operato del titolare/superiore gerarchico, nel caso di specie, per l'appunto, riverberava in ordine all'applicabilità o meno della fattispecie prevista e punita dall'art. 616 del

codice penale già sopra evidenziato.

Gli Ermellini, precisavano anzitutto come la specifica condotta di presa cognizione della corrispondenza poteva avvenire in assenza delle condotte di sottrazione o distrazione, solo con riferimento ad una corrispondenza “chiusa”. Del resto lo stesso legislatore “letteralmente” non lascia spazio ad interpretazioni :”Chiunque prende cognizione del contenuto di una corrispondenza chiusa..”.

A seguito di questa precisazione che escludeva l’applicazione dell’art. 616 codice penale alla corrispondenza aperta salvo che la stessa fosse stata oggetto di sottrazione o distrazione, restava alla Corte il problema di fornire una definizione di posta elettronica “chiusa”.

Nel caso di specie la Cassazione riteneva che la corrispondenza poteva essere definita "chiusa" nei confronti di coloro che non erano legittimati all'accesso al sistema informatico di ricezione e invio della posta elettronica. Secondo i Giudici della Corte era infatti la legittimazione all'uso del sistema informatico o telematico, derivante dalla proprietà o dalle norme che regolano l'uso dell'impianto, ad abilitare il singolo alla conoscenza delle informazioni in esso custodite. **In sintesi affermava che la corrispondenza in esso custodita è lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano delle credenziali di accesso, con la conseguenza che nei confronti di tali soggetti la corrispondenza non può ritenersi "chiusa".**

La Corte nello specifico osservava che quasi tutte le organizzazioni aziendali sono a conoscenza delle password poste a protezione dei computer e della corrispondenza di ciascun dipendente, prassi peraltro in linea con le previsioni in materia di protezione dei dati personali (provvedimento del Garante per la protezione dei dati personali dell'1 marzo 2007 n. 13 – Assenze del Personale) che autorizzano i dirigenti aziendali ad accedere ai computer in dotazione dei propri dipendenti, qualora, ovviamente, essi siano a conoscenza delle relative credenziali di accesso e, aggiungerei, il dipendente è informato di tale evenienza.

Appare evidente tuttavia come il concetto di posta “chiusa” nel caso di specie fosse ricondotto ad un particolare contesto connaturato da una titolarità di mezzi e proprietà del dominio non personale del dipendente e come l’utilizzo della email aziendali vieti l’utilizzo per scopi personali della stesse, con l’ulteriore conseguenza che verrebbe meno anche il requisito del “a lui non diretta”, volendo qui significare che la email al di là del ricevente specifico magari appartenente ad una specifica articolazione produttiva sarebbe logicamente diretta all’azienda e non al singolo dipendente. A ciò sia permesso poi aggiungere una considerazione pratica che vede anche nell’ambito della posta cartacea o tradizionale soprattutto in ambito aziendale la figura di una o più persone “autorizzate” ad aprire la corrispondenza comunque pervenuta anche a titolo “personale” al dirigente dell’articolazione.

Termini tuttavia molto “interpretabili” e facilmente contestabili, (aziendale/privato/personale/diretta/non diretta) in quanto anche nell’ambito di una corrispondenza “aziendale” potrebbero rilevarsi, talvolta, comunicazioni private e riservate. Invero, al di là della presa di posizione della Cassazione, si fatica ancora a dare una precisa definizione di email “aperta”/email “chiusa” scevra da alterne interpretazioni dottrinali e

giurisprudenziali. In merito alle mail aziendali “private” mi sia concesso, poi, un aneddoto; spesso capita di leggere mail definite “aziendali” perché scambiate all’interno di una realtà produttiva ma che nel contenuto superano di gran lunga i migliori scambi epistolari tra Giacomo Casanova e Manon Balletti.

Tornando seri, di recente è stata pubblicata
all’indirizzo
: http://www.gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca la circolare 1/2018 della Guardia di Finanza - Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali. Il Manuale aggiorna le direttive operative del Corpo concernenti l’esecuzione delle verifiche, dei controlli fiscali e delle indagini di polizia economico-finanziaria finalizzate al contrasto dell’evasione, dell’elusione e delle frodi fiscali.

Nello specificare, tra l’altro, che tutte le operazioni di acquisizione di materiale e/o supporti informatici devono svolgersi con l’assistenza di personale specializzato del soggetto ispezionato e sancire **il divieto di eseguire operazioni direttamente sugli apparati in uso al contribuente in assenza di un suo espresso consenso;** in relazione al tema qui in trattazione stabilisce:

“Per quanto riguarda le comunicazioni via e-mail, intercorse fra l’operatore ispezionato e soggetti terzi, ovvero fra articolazioni interne della stessa struttura imprenditoriale, occorre tenere presente le particolari disposizioni previste per l’acquisizione e l’esame di documentazione contenuta in plichi sigillati, o per la quale è opposto il segreto professionale, adattate alle prescrizioni dettate in tema di fatturazione e conservazione dei documenti in forma elettronica; per effetto delle richiamate previsioni, le comunicazioni via e-mail già “aperte” e visionate dal destinatario sono direttamente acquisibili dai verificatori, mentre quelle non ancora lette o per le quali è eccepito il segreto professionale possono essere acquisite sulla base di un provvedimento di autorizzazione dell’Autorità Giudiziaria, ex art. 52, comma 3, del D.P.R. n. 633/1972”.

Il comma 3 dell’art. 52 del D.P.R. n. 633/1972 precisa che:

“È in ogni caso necessaria l'autorizzazione del procuratore della Repubblica o dell'autorità giudiziaria più vicina per procedere durante l'accesso a perquisizioni personali e all'apertura coattiva di pieghi sigillati, borse, casseforti, mobili, ripostigli e simili e per l'esame di documenti e la richiesta di notizie relativamente ai quali è eccepito il segreto professionale, ferma restando la norma di cui all'articolo 103 del codice di procedura penale”.

Anche la circolare, è chiara nel definire due tipologie di email: quelle aperte e visionate e quelle non ancora lette, nel tentativo di abbandonare l’atavico dibattito “email aperta”/“email chiusa” dirotta la questione su email aperte e visionate (sarà interessante vederne l’eventuale etimologia ed interpretazione rispetto alla parola “lette”) ed email “non lette”. In ogni caso la soluzione fornita dalla circolare appare in ogni caso **la più solida ed illuminata,** pur richiedendo di individuare le email “chiuse” e chiedere comunque alla parte di provvedere ad “aprirle e visionarle”, ovvero rimuovere la notifica, di “non lette” dalle stesse,

indipendentemente dalla effettiva “apertura/lettura”.

Invero nella pratica, accade sovente di non dover ricorrere ad alcuno degli articoli su richiamati, in quanto la parte aderisce prontamente ad una apertura spontanea dei plichi facendone prendere visione agli operatori, consapevole che una sua eventuale opposizione alla richiesta di apertura innesterebbe comunque una più laboriosa procedura che comunque ed in ogni caso porterebbe ad una apertura coercitiva del plico. E parimenti accade che filtrate attraverso il client di posta elettronica quelle non “ancora lette” le stesse vengano con un “click” (segna come letto) aperte.

Va ricordato altresì che anche nell’ambito delle operazioni di polizia giudiziaria “strictu sensu” (mi sia concessa la sintesi) allorquando ci si trova dinanzi a “pieghi sigillati o altrimenti chiusi” la particolare procedura prevista dall’art. 353 del c.p.p sancisce:

1. *“Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.*
2. *Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata e l'accertamento del contenuto.*
3. *Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati”.*

Pur non essendo espresso così chiaramente come nell’art. 52 comma 3 del D.P.R. 633/72 è evidente come siffatta procedura sia richiesta solo allorquando si debba procedere ad una apertura “coattiva” ovvero contro la volontà della parte che si rifiuta, a richiesta, di aprire i plichi sigillati o altrimenti chiusi.

Tornado alle attività svolte dalla Guardia di Finanza e richiamate nella circolare summenzionata nel riconoscere la validità di quanto dettato dalla circolare in termini di “garanzie” riconosciute alla parte e ai militari che operano l’intervento, va evidenziato come nella pratica emergano tuttavia alcune criticità /difficoltà meritevoli a parere di chi scrive di essere considerate.

La prima attiene al mancato consenso da parte dell’interessato alla cosiddetta operazione “one click” ovvero filtra le email non lette e le segnala come lette. Talvolta soprattutto quando si ha a che fare con archivi di posta datati e risalenti nel tempo la controparte non sempre acconsente a fare le cose “in fretta” e preferisce un analisi “one by one”. Ora è logico ritenere che se detta operazione può essere effettuata su piccoli archivi o su un numero limitato di email le cose si complicano non poco quando trattasi di migliaia di mail, spesso non riconducibili ad un unico soggetto e che, per non farci mancare nulla, magari è anche fisicamente assente.

La seconda, è che spesso per ragioni non solo di tempo ma anche di praticità e operative (dettate dallo specifico caso) si rende necessario procedere all’acquisizione di interi archivi di posta:

- esportati di default periodicamente dal sistema;
- realizzati dall’utente per diversi scopi (storici, statistici, amministrativi etc.);
- realizzati all’atto dell’accesso su richiesta da parte della Guardia di Finanza.

Quanto ai primi due si tratta solitamente degli archivi più interessanti, atteso che le email periodicamente conservate “on line” dal sistema soprattutto in ambito aziendale sono relative a periodi recenti e limitati per ovvie ragioni di risparmio dello spazio dedicato sul server a ciascun dipendente e risultano essere le meno “determinanti” nell'ambito di controlli fiscali che risalgono spesso a bienni precedenti quello in corso.

Quanto alle ultime, ovvero quelle realizzate su richiesta da parte della Guardia di Finanza, è innegabile come spesso la parte acconsenta, nell’ottica di ricevere il minor disagio possibile dalle operazioni di accesso in corso, ad esportare per esempio nel caso di utilizzo di “Outlook”, un file .pst, contenente l’intero archivio di posta. O ancora si potrebbe decidere per motivi di opportunità di procedere all’acquisizione di tutti i file .pst presenti in locale su specifici personal computer o sul server dell’azienda.

In tutti questi casi è facile comprendere, soprattutto quando la mole di dati è rilevante, quali siano le difficoltà di procedere, preliminarmente all’acquisizione, ad un’analisi dettagliata dei singoli archivi alla ricerca di eventuali email “chiuse” che andrebbero aperte a cura dell’intestatario della casella email corrispondente.

Una soluzione potrebbe consistere in un “congelamento” del dato attraverso la copia dei file nel caso di esempio .pst su idonei supporti nel numero di almeno due (una copia garanzia e una copia lavoro) dopo aver provveduto alla compressione in archivi .zip di ciascun file o gruppi di file e ciò al fine di preservare ulteriormente da accidentali modifiche i file .pst, che all’atto della loro apertura potrebbero essere modificati, si procederà quindi nel rispetto delle prescrizioni dettate in materia di digital forensic quanto al calcolo dell’algoritmo di hash per ciascun file .zip. Tale congelamento permetterebbe da un lato agli investigatori di conservare lo stato delle cose, dall’altro riservare in un secondo momento e con tempi congrui l’analisi di detti file alla ricerca ed individuazione delle sole email d’interesse previa apertura/visione di quelle non ancora lette.

In subordine, la parte potrebbe rilasciare apposita delega/autorizzazione scritta ad effettuare anche in sua assenza l’esame delle email e procedere alla lettura anche di quelle non ancora lette, su suo espresso consenso.

Questa potrebbe essere una soluzione capace di contemperare le contrapposte esigenze, degli attori coinvolti, nell’evidenza che ciò che a volte può apparire di facile soluzione con pochi “click”, ma nella realtà operativa non lo è!

Concludo con un'ulteriore osservazione attinente il fatto, al di là della facilità di modifica delle notifiche di stato letta\non letta di una mail, ritengo che anche il fatto di leggere e poi spuntare

come non letta la stessa email equivalga ad una volontà espressa del destinatario a far risultare quella email come non letta e come tale debba essere considerata da chi vorrà acquisirla.

Note

[1] https://www.ilfattoquotidiano.it/2013/08/14/google-chi-usa-gmail-non-puo-pretendere-rispetto-della-privacy/684885/

[2] G.Costabile, G. Mazzaraco, F.Cajani – Computer Forensics e Indagini Digitali – Manuale tecnico giuridico e casi pratici – Volume II Capitolo 7 pag. 275 e ss. - Experta 2011

[3] https://www.mailstore.com/en/products/

[4] https://takeout.google.com/settings/takeout?pli=1

A cura di: **Pier Luca Toselli**