Pec DA USARE CON CURA

DI **GIUSEPPE CARAVITA**

«A volte perdiamo i pomeriggi a cercare quella maledetta "cartolina" di una raccomandata spedita al collega e finita nel fascicolo sbagliato. Ora invece potremo tenere tutto sul pc e ricercarle subito. E non è un vantaggio da poco». Pierluigi Perri, avvocato, non sarà il solo a passare alla Pec, posta elettronica certificata, dal prossimo 28 novembre. Punto di partenza, secondo il decreto anticrisi, di un percorso di migrazione dalle vecchie raccomandate cartacee che dovrebbe coinvolgere, almeno sulla carta, due milioni di professionisti iscritti agli albi (avvocati, notai, architetti ecc), le imprese di nuova costituzione e poi, a gradi, entro il 2011, tutte le aziende.

Molti hanno paura della Pec, altri invece guardano con un certo ottimismo a questa forma di posta elettronica "sicura" e caratterizzata da avvisi ufficiali di invio e poi di recapito al destinatario, concettualmente simili alle vecchie "cartoline" recapitate dal postino.

Ma qual è la reale robustezza informatica della Pec? Il sistema, che già conta mezzo milione di caselle ed è in fase di rodaggio da più di cinque anni, è in pratica (e in gergo) una rete di caselle postali separata dalla internet normale. La ventina di gestori accreditati al servizio Pec dal Cnipa hanno tutti dominii riservati per la Pec, e il valore legale di un documento scatta solo se inviato a un'altra casella Pec. In modo poi non anonimo. «Ogni utente è registrato, sia esso persona fisica o giuridica - spiega Marco Parisi di Telecom Italia - e la procedura di accredito è verificata dal Cnipa».

Tecnicamente ogni provider Pec ha una sua "firma digitale" registrata presso le 16 *certification authority* delegate dal Cnipa. «Questo significa che ogni messaggio in partenza da una nostra casella Pec - continua Parisi - viene "imbustato" e certificato con firma digitale. La busta è riconosciuta dal provider di destinazione, anch'esso fornitore di Pec. L'intero processo è "tracciato" in una serie di log (file di registrazione) che riportano data, orario, dimensioni, stato del documento». E la legge impone che i provider conservino tutte le documentazioni per almeno 30 mesi.

Non solo: i provider sono tenuti a filtrare preventivamente i messaggi e gli allegati dai virus e non accettare sulle caselle Pec messaggi non certificati (quindi anche di spam). Invece possono inoltrare, anche su caselle email normali o persino su sms, notifiche di arrivo dei messaggi.

Un sistema di dominii internet a parte, quindi, il mondo Pec. «Persino gli indirizzi Pec non saranno disponibili su una directory pubblica, proprio per evitare ogni intromissione», conclude Parisi.

Inoltre, su molti documenti legali, gli utenti già usano proprie firme digitali, riconosciute dal sistema di 16 certificatori che fa capo al Cnipa. Tutto bene dunque? «Sì e no - rileva Danilo Bruschi, docente di sicurezza informatica all'Università degli Studi di Milano – nella firma digitale si usano oggi algoritmi Res da 1024 bit, provati e riprovati e ragionevolmente sicuri. Credo che per almeno dieci anni su questi si possa stare tranquilli. Il problema invece è che la Pec è comunque una webmail con documenti in chiaro, residenti su un server, per quanto sicuro si pretenda, ma esterno. Molti documenti sono di tipo riservato, e personalmente non vedo altra soluzione che cifrarli». Ma questa seria criticità richiede di ottenere ogni volta la chiave pubblica (per esempio Pgp) dal destinatario.

Certo, i provider garantiscono la protezione di ogni casella Pec con password e altro «ma il rischio di intrusione resta non nullo - continua Bruschi - come ci insegna la storia anche recente della security informatica in Italia».

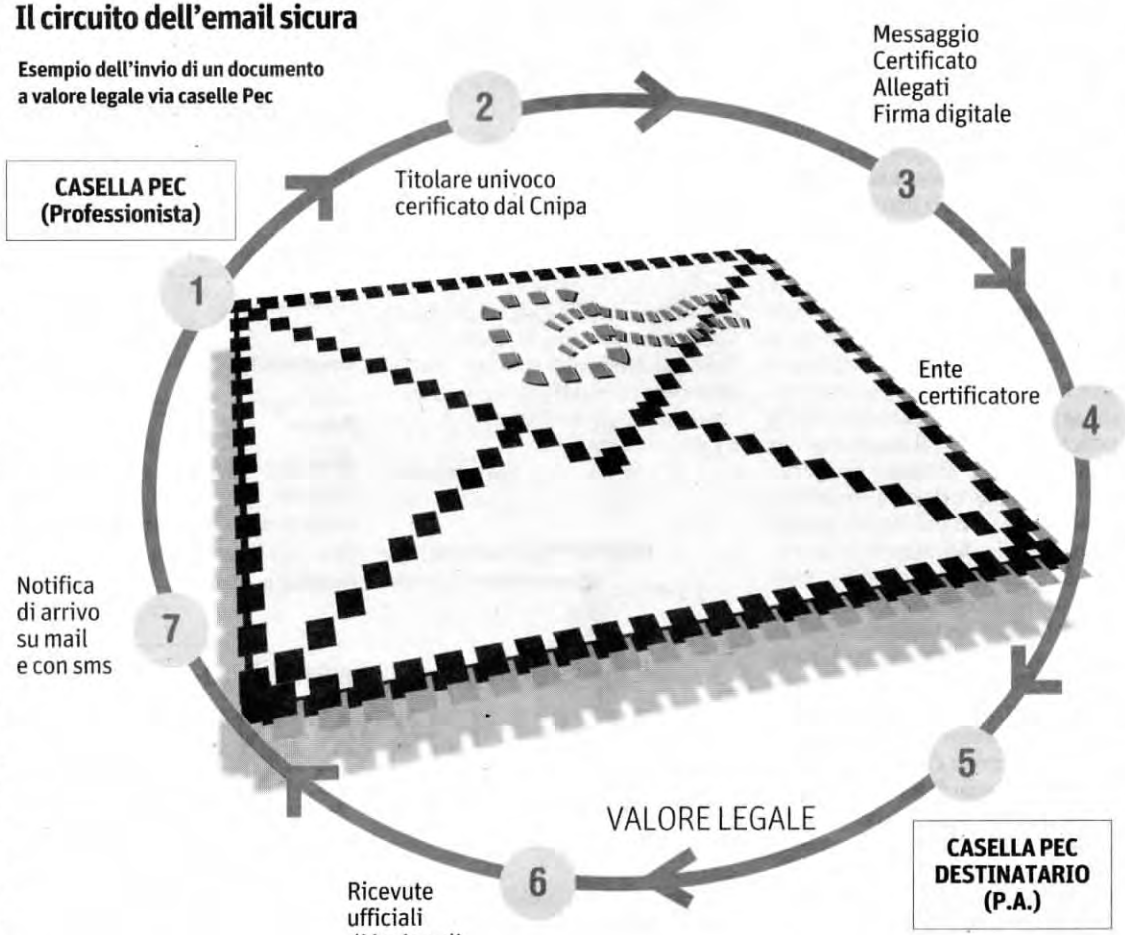
Che fare? «Accettarla e usarla facendo un bilancio tra rischi e vantaggi. Un buon sistema di archiviazione dei documenti aziendali è necessario - osserva Perri - e sulla Pec, che per prima in Italia si sperimenterà su milioni di utenze, si potranno impiantare applicazioni aggiuntive. Come un intero studio legale a fascicoli elettronici accessibile sul palmare».

© RIPRODUZIONE RISERVATA

Le caselle di posta certificata sono separate da internet Ma il rischio non è escluso al 100%

Il circuito dell'email sicura

Esempio dell'invio di un documento a valore legale via caselle Pec



CRITTARE I DATI PER TUTELARSI DI PIÙ

La busta e il contenuto viaggiano «in chiaro» Meglio proteggersi con software, anche open

DI **ANDREA MONTI**

L'avvicinarsi della data in cui la posta elettronica certificata (Pec) diventa obbligatoria per aziende e professionisti pone con sempre maggiore urgenza la necessità di rispondere a domande che, da tempo, sono rimaste senza risposta.

Partiamo dal "valore" di un messaggio Pec. Al contrario di quanto si pensa comunemente, la Pec fa solo fede sulla data di invio e ricezione di un messaggio, ma – giuridicamente – non ne imputa il contenuto al suo autore. Per questo secondo risultato è necessario applicare al messaggio una firma elettronica qualificata. Tutto questo, però, non risolve il problema della confidenzialità del messaggio.

Sia la «busta elettronica» (la componente Pec del messaggio) sia il contenuto firmato elettronicamente, infatti, viaggiano e sono custoditi "in chiaro". Non sono – in altri termini – cifrati e somigliano molto più a una cartolina postale che a una lettera raccomandata. Dunque, chi volesse garantirsi anche la riservatezza delle comunicazioni dovrà ricorrere a software crittografici, come i due noti prodotti open source Gpg e TrueCrypt. A questo proposito, detto per inciso, sarebbe interessante conoscere il parere degli ordini professionali (e in particolare di quelli di medici e avvocati) i cui iscritti sono costretti a lasciare la propria corrispondenza elettronica con valore legale e relativa a dati spesso sensibilissimi su server di terze parti senza che, obbligatoriamente, questi dati siano protetti dalla cognizione abusiva.

Per usare la Pec con un minimo di sicurezza, dunque, un soggetto dovrebbe servirsi contemporaneamente di almeno tre applicazioni (client Pec, client per la firma elettronica, applicazione crittografica) e sperare che il proprio corrispondente faccia lo stesso.

L'assenza di una decisione a monte da parte del Cnipa sul punto rischia di generare una vera e propria babele o – al contrario – una sostanziale esposizione a rischio dei dati personali di milioni di persone.

A valle di tutto questo, non va trascurata la componente economica per quanto riguarda i costi indiretti che non necessariamente bilanciano le economie rappresentate dalla *paperless-mail*. Già una volta, negli anni Ottanta, il marketing It cercò di convincere il mondo che della carta si poteva fare a meno. Con buona pace degli alfieri del *paperless-office*, ora più che mai il mondo è sommerso dalla carta e le cose non cambieranno significativamente con la Pec. I messaggi – specie nella pubblica amministrazione – continueranno a essere stampati «a scanso di equivoci»; e se anche la carta venisse messa fuori gioco, non risultano stime concrete del costo (anche in termini ambientali) dello storage necessario per memorizzare l'enorme quantità di dati generati dalla Pec.

© RIPRODUZIONE RISERVATA

10 mln

LE CASELLE DELLA PEC
Al 29 novembre 2011, a migrazione completata, si stimano oltre 10 milioni di caselle postali Pec attive in Italia.

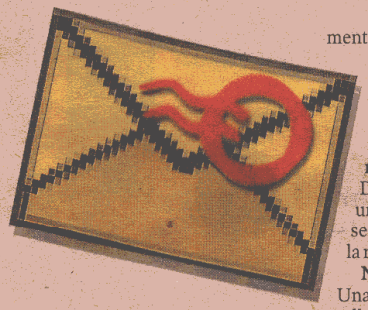
FASCICOLI DIGITALI
I sistemi di archiviazione professionali potranno dotarsi di programmi integrati alle caselle Pec, come i fascicoli digitali.

LE FORME DELLA FIRMA
La firma digitale, prima solo su smart card, verrà offerta su soluzioni "tutto web" o su chiavetta elettronica.

A PROPOSITO DI PEC da MOVA di Sole 24 ore

>documenti>Pubblica amministrazione>**criticità**

UNA PEC **senza** IDENTITÀ



È scattato da pochi giorni l'obbligo per i professionisti di dotarsi di una casella di posta elettronica certificata. Ma ancora non si sono dissipati i dubbi sui problemi e i rischi connessi alla Pec.

Carenza di identificazione. Non esiste – come nella firma digitale – l'obbligo di identificare con certezza il richiedente di Pec, e infatti ci sono diversi metodi per ottenerne una. Alcuni fanno firmare un documento cartaceo. Altri dematerializzano il processo, affidando l'identificazione del contraente alla richiesta di una mailbox non Pec, allo strumento di pagamento (carta di credito) e all'invio tramite fax del documento di identità. In astratto questo non sembra sufficiente a scongiurare furti di identità. È un'ipotesi ovviamente patologica ma possibile, e che sarebbe stata scongiurata semplicemente obbligando all'uso della firma digitale.

Scopo limitato. La Pec serve solo per attestare data di invio e ricezione di un messaggio.

Validità del messaggio. La Pec valida la "busta", la firma digitale del mittente il "foglio" contenuto all'interno (è vero che la ricevuta torna con la firma digitale del gestore, ma se manca quella del mittente, il documento non è attribuibile giuridicamente a quest'ultimo).

Valore probatorio. Chi dichiara di non avere ricevuto il messaggio quando l'altra parte esibisce la ricevuta di consegna, non può limitarsi a "fare catenaccio" negando la circostanza. D'altra parte, sarebbe possibile una verifica presso il gestore del servizio che è tenuto a conservare la ricevuta in questione.

Niente compiuta giacenza. Una Pec è ricevuta quando arriva nella casella di posta del gestore del servizio, non quando viene letta dal destinatario.

Sicurezza. La Pec gira in rete con protocolli sicuri, ma è memorizzata sui server dei gestori senza protezione crittografica (l'Assocertificatori fa notare in proposito però che i gestori hanno comunque una responsabilità sulla sicurezza dei dati e sono soggetti alla vigilanza del Cnipa, *ndr*).

Standard non riconosciuto. La Pec non è standard a livello internazionale (anche se usa protocolli che lo sono).

Total cost of ownership. Per grandi volumi, andrebbe calcolato il costo dello storage e delle altre misure di sicurezza per evitare perdite di dati.

"Denial-of-service" per la Pa. Con la Pec si possono inviare pressoché contemporaneamente un numero molto rilevante di richieste che implicano l'apertura di altrettanti procedimenti amministrativi. Questi saranno tutti assoggettati allo stesso termine di legge per la loro conclusione e in assenza di un'efficiente organizzazione di "backoffice" il rischio è la paralisi.

Proliferazione e caos. Se, come pare, i cittadini potranno parlare con la Pa solo usando la Pec attribuita dallo specifico ente, il grado di confusione per i cittadini potrebbe essere ingestibile.

Andrea Monti

© RIPRODUZIONE RISERVATA