Lo strano caso di una firma digitale in crisi d'identità

(Brevi riflessioni sulla Circolare n. 10/2009 del Ministero del Lavoro, della Salute e delle Politiche Sociali)[1]

di Avv. Marco Scialdone

Con circolare n. 10/2009 il Ministero del Lavoro, della Salute e delle Politiche Sociali ha fornito le istruzioni operative per la trasmissione telematica delle autocertificazioni relative alla non commissione degli illeciti ostativi al rilascio del Documento Unico di Regolarità Contributiva (DURC), ovvero al decorso dei tempi previsti per ciascun illecito dal Decreto Ministeriale 24 ottobre 2007.

Viene richiesta la compilazione di un modulo predisposto dal Ministero da firmarsi digitalmente e da inviarsi per e-mail o posta elettronica certificata, unitamente ad un'immagine scannerizzata di un documento di identità in corso di validità.

Nel prosieguo della trattazione si cercherà di argomentare per quali ragioni la procedura da ultimo richiamata - limitatamente all'obbligo di allegazione dell'immagine scannerizzata del documento d'identità - risulti in contrasto con le disposizioni del d.lgs 82/2005 e s.m.i. (c.d. Codice dell'Amministrazione Digitale – CAD), ignorando, altresì, la natura della firma digitale e la sua ontologica diversità rispetto alla firma autografa.

Occorre prendere le mosse da quanto disposto dal D.P.R. 445/2000 (Testo Unico in materia di documentazione amministrativa – T.U.D.A.) in materia di "autocertificazioni" (*rectius*, dichiarazioni sostitutive). In particolare, l'articolo 47 così recita: *"L'atto di notorietà concernente stati, qualità personali o fatti che siano a diretta conoscenza dell'interessato è sostituito da dichiarazione resa e sottoscritta dal medesimo con la osservanza delle modalità di cui all'articolo 38"*. Tale ultima disposizione prevede, al terzo comma, che *"le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero* ***sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate per via telematica****; nei procedimenti di aggiudicazione di contratti pubblici, detta facoltà e' consentita nei limiti stabiliti dal regolamento di cui all'articolo 15, comma 2 della legge 15 marzo 1997, n. 59"*.

La ragion d'essere dell'obbligo di allegazione della copia fotostatica del documento di identità del firmatario è ben chiarita in una recente pronuncia del Consiglio di Stato[2], allorquando si afferma che

---

[2] CONSIGLIO DI STATO, SEZ. VI - sentenza 23 luglio 2008 n. 3651. Trattasi di un orientamento consolidato: cfr., *ex plurimis*, CONSIGLIO DI STATO, SEZ. V - sentenza 7 novembre 2007 n. 5761 *"Ai sensi del combinato-disposto degli artt. 21, comma 1° e 38, commi 2° e 3° del D.P.R. n. 445 del 2000, l'allegazione della copia fotostatica, sia pure non autenticata, del documento di identità dell'interessato vale a conferire legale autenticità alla sua sottoscrizione apposta in calce ad una istanza o ad una dichiarazione, e non rappresenta un vuoto formalismo ma semmai si configura come l'elemento della fattispecie normativa diretto a comprovare, oltre alle generalità del dichiarante, l'imprescindibile nesso di imputabilità soggettiva della dichiarazione ad una determinata persona fisica"*.

esso *"si configura come l'elemento della fattispecie normativa diretto a comprovare, oltre alle generalità del dichiarante, l'imprescindibile nesso di imputabilità soggettiva della dichiarazione a una determinata persona fisica"*.

Non si tratta, dunque, di un vuoto formalismo ma, al contrario, dello strumento che consente, unitamente alla sottoscrizione autografa, di raggiungere una ragionevole certezza circa la provenienza soggettiva della dichiarazione.

Orbene, il nesso di imputabilità soggettiva cui il Consiglio di Stato fa riferimento è, nel caso del documento informatico firmato digitalmente, insito nella firma stessa per la diversa natura della "sottoscrizione" digitale rispetto a quella autografa.

La firma digitale è definita dal Codice dell'Amministrazione Digitale come un *"particolare tipo di firma elettronica qualificata*[3] *basato su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare l'autenticità e l'integrità di un documento informatico o di un insieme di documenti informatici"*.

Secondo quanto stabilito, poi, dall'art. 24, comma 1, CAD, la firma digitale deve riferirsi in maniera univoca ad un solo soggetto e al documento o all'insieme dei documenti cui è apposta o associata: per la sua generazione occorre un certificato qualificato[4] che, al momento della sottoscrizione, non risulti scaduto, revocato o sospeso.

Attraverso il certificato devono rilevarsi gli elementi identificativi del titolare e del certificatore (nonché gli eventuali limiti d'uso) tant'è che la legge pone a loro carico due obblighi speculari: da un lato, il certificatore ha l'obbligo di provvedere con certezza all'identificazione della persona che fa richiesta della certificazione, dall'altro il titolare del certificato ha l'obbligo di assicurare la custodia del dispositivo di firma e di adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri, nonché di usarlo personalmente.

Da tali disposizioni emerge con chiarezza quale passaggio epocale la firma digitale abbia segnato in ragione delle sue peculiarità, del suo essere "altro" rispetto alla firma autografa. Un individuo può

---

[3] L'articolo 1, lett. r) CAD definisce la firma elettronica qualificata come *"la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma"*.

[4] L'articolo 28 CAD prevede esplicitamente che i certificati qualificati debbono contenere almeno le seguenti informazioni:

a. indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b. numero di serie o altro codice identificativo del certificato;
c. nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
d. nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;
e. dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f. indicazione del termine iniziale e finale del periodo di validità del certificato;
g. firma elettronica del certificatore che ha rilasciato il certificato realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

sottoscrivere infiniti documenti cartacei e la sua firma sarà sempre uguale a se stessa perché legata alla fisicità del sottoscrivente, laddove la firma digitale sarà sempre diversa perché originata a partire dal contenuto del documento.

Si può dire che mentre la firma autografa è orientata all'individuo, la firma digitale è orientata al documento.

Ciò innesca dinamiche giuridiche del tutto nuove, prima fra tutte, l'esigenza di un soggetto, terza parte fidata (leggasi: il certificatore) che attesti la nostra identità, attesti in sostanza "chi siamo" in ambiente digitale. Mentre nei sistemi tradizionali di firma è l'autografia a farsi portavoce e garante della nostra identità, il carattere inevitabilmente neutro dei bit pone un'esigenza ulteriore che è quella legata all'identificazione del soggetto firmatario, esigenza che, come abbiamo visto, è soddisfatta attraverso l'intervento di una terza parte, il certificatore, che "garantisce" circa la nostra identità nei rapporti con i terzi.

Vi è di più: il legislatore ha reputato talmente delicato il ruolo del certificatore da arrivare a sanzionarne penalmente la condotta allorquando, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato[5]. Specularmente, ha sanzionato penalmente la condotta di chi dichiari o attesti falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona[6].

Alla luce delle considerazioni sopra esposte dovrebbe apparire di tutta evidenza come l'obbligo di allegazione dell'immagine scannerizzata di un documento d'identità sia da considerarsi inutile nel caso in cui la dichiarazione sostitutiva sia sottoscritta digitalmente, in caso contrario, ciò equivarrebbe a un vuoto formalismo, del tutto irrilevante rispetto all'imputazione soggettiva dell'atto.

Tuttavia, il contenuto della circolare 10/2009 non si limita ad essere *"illogico"* ma è altresì *contra legem*, giacchè si pone in aperto contrasto con il contenuto dell'articolo 65, comma 1, lett. a) del CAD che così recita: *"Le istanze e le dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica ai sensi dell'articolo 38, comma 1 e 3, del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 sono valide:* ***a) Se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato****"*.

Dunque, è la stessa disposizione di legge a chiarire che, allorquando la dichiarazione venga firmata digitalmente, non sia necessario presentare unitamente copia fotostatica del documento d'identità. L'unica formalità richiesta è che la firma digitale sia basata su certificato rilasciato da un certificatore

---

[5] Art. 640-quinquies C.P. – *(Frode informatica del soggetto che presta servizi di certificazione di firma elettronica). – "Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro"*.

[6] Art. 495-*bis*. C.P. – *(Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri)*. – Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno.

accreditato ex art 27 CAD[7] e, dunque, in possesso dei requisiti del livello più elevato in termini di qualità e sicurezza.

Infine, occorre dedicare qualche parola alle modalità di trasmissione del documento informatico individuate dalla circolare: si afferma espressamente che *"il file firmato digitalmente dovrà essere inviato per email o posta elettronica certificata"*, indicando, successivamente, solo un indirizzo di posta elettronica certificata (PEC).

Sembra, dunque, suggerirsi una perfetta interoperabilità tra il sistema di posta elettronica certificata e quello di posta elettronica tradizionale, cosicchè l'indirizzo PEC indicato risulti idoneo alla ricezione di posta elettronica "ordinaria".

Ciò non corrisponde al vero.

E' lo stesso Centro Nazionale per l'Informatica nella Pubblica Amministrazione – CNIPA, ovverosia l'autorità preposta alla tenuta dell'elenco dei soggetti abilitati a fornire il servizio di posta elettronica certificata, ad affermare in una sua pubblicazione ufficiale: *"È importante sottolineare che il servizio di Posta Elettronica Certificata è "completo", ovvero produce le certificazioni – a valore legale – attestanti l'invio e la consegna di un messaggio,* ***solo se entrambi gli interlocutori dispongono di caselle PEC****, anche facenti capo a Gestori diversi (dovendo i vari Gestori garantire l'interoperabilità dei servizi offerti). Contrariamente, qualora da una casella di*

---

[7] *Articolo 29 CAD – Accreditamento*

1. *I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.*
2. *Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.*
3. *Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:*
    a. *avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;*
    b. *garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.*
4. *La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.*
5. *Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.*
6. *A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.*
7. *Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.*
8. *Sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE.*
9. *Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.*

PEC si spedisca un messaggio ad un destinatario che non ha una casella di posta certificata, l'unica ricevuta prodotta dal sistema è quella di accettazione, proveniente dal Gestore del mittente. Infine, ***qualora un messaggio di posta elettronica ordinaria venga spedito ad un destinatario PEC possono presentarsi due distinte situazioni: il messaggio non viene accettato dal Gestore e quindi non arriva al destinatario****, ovvero il messaggio entra nel sistema PEC e giunge al destinatario all'interno di una busta di anomalia (per maggiori dettagli si rimanda alle Regole Tecniche allegate al Decreto Ministeriale 2 novembre 2005).* ***I criteri per la gestione della posta elettronica ordinaria sono a discrezione del Gestore*** *(che deve comunque comunicarli ai propri utenti)* ***il quale potrebbe decidere, ad esempio per limitare il dannoso fenomeno dello spam, di non accettare messaggi provenienti da domini non PEC***"[8]

Lungi, dunque, dal potersi riscontrare una perfetta interoperabilità tra i due sistemi, si è in presenza di un quadro frammentato ed incerto, nel quale il messaggio inviato da una casella di posta elettronica ordinaria ed indirizzato, ad esempio, alla casella di posta elettronica certificata indicata nella Circolare potrebbe addirittura risultare non ricevibile e, nell'ipotesi più grottesca, essere automaticamente etichettato come spam.

Infine, a complicare ulteriormente il quadro, si inseriscono le disposizioni dell'art. 16, D.L. 185/2008, convertito in legge 2/2009, commi 6, 7, 8 e 9, con le quali si è introdotto del nostro ordinamento un principio di equivalenza tra la Posta Elettronica Certificata e un non meglio precisato "*indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali*".

In estrema sintesi, alle imprese e ai professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, viene riconosciuto il diritto di interloquire con la Pubblica Amministrazione, in via telematica, attraverso l'uno o l'altro sistema di comunicazione (dunque, si potrebbe finanche sostenere che esiste un diritto a non usare la PEC).

Cosa succede se un'impresa che si sia dotata di "*indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali*" voglia comunicare con una Pubblica Amministrazione che, come in questo caso, metta a disposizione esclusivamente un indirizzo PEC?

Difficile rispondere, l'unica cosa certa è che il problema deve essere saltato agli occhi del legislatore che nel Disegno di Legge recante "*Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*" (atto Senato n. 1082-b[9]), approvato in via definitiva nella giornata del 26 maggio u.s. e in attesa di pubblicazione in Gazzetta Ufficiale, ha inserito, all'articolo 35, una disposizione che così recita: *"1. Entro sei mesi dalla data di entrata in vigore della presente legge, il Governo adotta, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, e successive modificazioni, un regolamento recante modifiche al regolamento di cui al decreto del Presidente della Repubblica 11 febbraio2005, n. 68,* ***anche al fine di garantire l'interoperabilità del sistema di posta elettronica certificata con analoghi sistemi internazionali***".

Lunga e tortuosa è la strada verso l'Amministrazione Digitale.

---

8 Cfr. CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione, *La Posta Elettronica Certificata*, pag. 17, disponibile al seguente indirizzo: http://www.cnipa.gov.it/site/_files/cnipa_minig_11_alta.pdf (consultato il 10 maggio 2009)

9 Il testo è disponibile al seguente indirizzo: http://www.senato.it/service/PDF/PDFServer/BGT/00413067.pdf