



Dott. Roberto Alma

Roma, 5 dicembre 2011

Spett.le

Avv. Enzo Fogliani

Via mail

Gentili signori,

con riferimento alla Vs. missiva del 25 novembre 2011, troverete qui di seguito il parere da Voi richiesto in merito alla efficacia e validità dei Servizi di certificazione dell'oggetto del contratto offerto da Elaborazioni Digitali S.r.L ai propri clienti, (d'ora innanzi, per brevità, denominato anche il "Servizio").

In linea generale si può concludere che tale servizio assolve pienamente sia alla funzione di certificare l'oggetto del contratto (attribuendo data certa alla relativa stipulazione) sia alla funzione di consentire al consumatore di apporre una sottoscrizione elettronica valida a tutti gli effetti di legge, pur nell'assenza dell'utilizzo di un dispositivo di firma digitale.

Ciò detto, al fine di illustrare come tale conclusione sia stata raggiunta, occorre richiamare, in linea generale, la disciplina sulla stipulazione dei contratti attraverso internet, con particolare riferimento alle ipotesi rientranti nella categoria dei contratti del **commercio elettronico** (cd. *e-commerce*) di cui alla normativa contenuta nel D.lgs 9 aprile 2003, n. 70, intesi come quei contratti in cui la fase prenegoziale e quella negoziale si svolgono attraverso un sito internet predisposto al fine specifico di commercializzare beni e/o servizi (con esclusione, pertanto, degli altri contratti telematici¹ - quali, a titolo esemplificativo, i contratti conclusi mediante scambio di messaggi di posta elettronica).

¹ Sul punto V. SCORZA G., *Il contratto del commercio elettronico*, in CASSANO G., CIMINO P. I., *Diritto dell'internet e delle nuove tecnologie telematiche*, CEDAM, 2009, p. 138. Per la definizione di *contratto telematico*, inteso come il *contratto concluso mediante la trasmissione di dati informatizzati tra due computers connessi (non necessariamente tramite il web)*, ossia *l'accordo tra soggetti che utilizzano computers (o altri strumenti informatici) tra loro collegati e che sono, dunque, reciprocamente assenti (contratto inter absentes)*, V. FRANCESCHELLI V., *Il contratto virtuale. Diritto nel cyberspazio*, in *Contratti*, 1995, p. 569 e cfr. TOSI E., *Contrattazione telematica e conclusione del contratto virtuale*, in ROSSELLO C., FINOCCHIARO G., e TOSI E., (a cura di) *Commercio elettronico, documento informatico e firma digitale, la nuova disciplina*, Torino, pp. 97 ss.



Dott. Roberto Alma

A tal riguardo, sembra doveroso rilevare che né il Decreto Legislativo n. 70 del 2003 né, tantomeno, il Codice del Consumo dettano specifiche norme in materia di conclusione del contratto²: l'art. 13 del Decreto Legislativo 9 Aprile 2003, n. 70 si limita, infatti, a prevedere l'applicabilità delle norme generali sulla conclusione dei contratti *anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica*.

Occorre, pertanto, comprendere, in primo luogo, quale sia il momento effettivo di conclusione del contratto di *e-commerce*.

La risposta al suddetto interrogativo potrà - dal momento che il Fornitore ha, generalmente, una pluralità di schemi negoziali a disposizione³ - essere data esclusivamente *on a case by case basis*, previa analisi delle caratteristiche specifiche delle varie piattaforme di *e-commerce* sulle quali verrà implementato il Servizio di certificazione dell'oggetto del contratto qui esaminato.

In linea generale, tuttavia - sulla scia dell'opinione condivisa dalla maggioranza della dottrina - si può affermare che alla stragrande maggioranza dei servizi di *e-commerce* (in cui il Fornitore presenta i beni o servizi, indicando termini e condizioni di acquisto e approntando procedure e modulistiche automatiche da utilizzare per la trasmissione dell'ordine) sarà applicabile lo schema negoziale dell'**offerta al pubblico** ex art. 1336 c.c., con il conseguente perfezionamento del contratto nel momento in cui il venditore abbia conoscenza dell'accettazione dell'acquirente⁴.

² Una specifica disciplina sulla conclusione del contratto era, invece, contenuta nell'originario schema di Direttiva 31/2000/UE sul commercio elettronico, trasmesso dal Parlamento al Consiglio, in quanto il relativo art. 11 prevedeva espressamente che il contratto doveva considerarsi concluso nel momento in cui il destinatario del servizio ha ricevuto dal prestatore, per via elettronica, l'avviso di ricevimento della propria accettazione.

³ Per un'analisi approfondita degli schemi negoziali del commercio elettronico, V. PERLINGIERI G., *Il contratto telematico*, in VALENTINO D., (a cura di), *Manuale di Diritto dell'informatica*, Napoli, Edizioni Scientifiche Italiane, seconda edizione, 2011, pp. 265 ss., in cui si distingue tra **schema tradizionale** ex art. 1326 e 1335 c.c. (i.e scambio di e-mail), **offerta al pubblico** ex art. 1336 c.c., **invito ad offrire** e **accettazione per comportamento concludente** ex art. 1333 c.c.

⁴ Cfr. *ex plurimis*, SCANNICCHI, cit in SCORZA G., *Il contratto del commercio elettronico*, in CASSANO G., CIMINO P. I., *Diritto dell'internet e delle nuove tecnologie telematiche*, CEDAM, 2009, p. 165. Secondo PERLINGIERI G., *op cit.*, il **discrimen** tra **offerta al pubblico** ed **invito ad offrire** deve essere ravvisato nel fatto che nel secondo caso la dichiarazione negoziale è manchevole di uno degli elementi richiesti, risultando, pertanto, insuscettibile di accettazione poiché, sul piano oggettivo, non è idonea a prefigurare il contenuto dispositivo dell'accordo. In senso conforme PERLINGIERI G., *op cit.*; PENNASILICO M., *La conclusione dei contratti on-line tra continuità e innovazione*, in Riv. Dir. Inf., 2004, VI, pp. 805 ss.; *Contra cfr.*, *ex plurimis*, GAMBINO A. M., *L'accordo telematico*, Milano, 1997, pp. 141 ss.; DELFINI F., *Il D.P.R. 513/1997 e il*



Dott. Roberto Alma

Secondo la disposizione da ultimo richiamata, invero, l'Utente/Consumatore può semplicemente aderire o rifiutare la proposta pubblicizzata dall'imprenditore tramite la digitazione del *tasto negoziale* (cd. *point and click*), ciò che implica, infatti, l'imputazione della volontà al soggetto al quale è riconducibile il *click*.

Appare, al riguardo, doveroso precisare che ai sensi dell'art. 13, comma secondo del citato D.lgs, 70/2003, il Fornitore è tenuto ad *accusare ricevuta* dell'ordine del destinatario, (fornendo un riepilogo delle condizioni generali del contratto, delle informazioni relative alle caratteristiche essenziali del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili), ciò che induce a ritenere che si tratti di una mera conferma di un contratto già perfezionato *inter partes*⁵, con l'evidente *ratio* di fornire al consumatore una "prova" dei termini dell'accordo da esibire in un eventuale giudizio⁶.

contratto telematico, in *Contratti*, 1998, p. 297 ss; GIOVA S., *La conclusione del contratto via internet, Evoluzione tra normativa e prassi*, Napoli, 2000, pp. 89 ss.; CAVALAGLIO L., *L'art. 11 della Direttiva 2000/31/CE* in Riv. Dir. Inf. 2001, pp. 105 ss., secondo i quali il momento effettivo della conclusione del contratto di *e-commerce* dovrebbe, invece, essere ravvisato nella trasmissione effettiva dell'ordine completo del numero di carta di credito. In senso critico V. PERLINGIERI G., *op cit.*, secondo cui la digitazione del numero di carta di credito non equivale ad *inizio della esecuzione* ex art. 1327 c.c., in quanto non è pagamento né rilascio di un mezzo di pagamento, bensì mera autorizzazione a riscuotere presso l'emittente della carta, con ciò, quindi, implicando una semplice *conferma* di un'accettazione del cliente già esistente. In senso conforme V. DENOVA G., *Un contratto di consumo via Internet*, in *Contratti*, p. 114; OPPO G., *Disumanizzazione del contratto?* In Riv. Dir. Civ, 1998, I, p. 531.

⁵ V. sul punto PENNASILICO M., *op cit.*, pp. 810-811, il quale ritiene che l'invio della ricevuta dell'ordine non incida sulla conclusione del contratto che, di regola, è concluso nel momento e nel luogo nei quali l'accettazione dell'oblato giunge all'indirizzo telematico del preponente, quindi, in un momento anteriore all'invio della ricevuta in questione, costituendo, quindi, un obbligo accessorio e successivo all'accordo. V. anche TOSI E., *Contrattazione telematica e conclusione del contratto virtuale*, cit., pp. 108 ss. In senso parzialmente critico V. PENNALISTICO M., *op cit.*, pp. 817 ss., secondo cui la contrattazione *on line* potrebbe anche non essere perfettamente ricondotta ad uno degli schemi negoziali previsti dall'art. 1326 ss. c.c., potendosi, ad esempio, ammettere che *la ricevuta dell'ordine di acquisto sia trasformata, per effetto di una clausola negoziale, da obbligo post contrattuale del venditore ad atto finale del procedimento formativo del contratto, la cui sequenza sarà rappresentata dalla formula: offerta al pubblico + inoltro dell'ordine + conferma dell'ordine*. *Contra* V. IASELLI M., *Diritto e nuove tecnologie*, Altalex editore, 2011, p. 271, il quale ritiene che il contratto si perfezioni solo nel momento in cui il consumatore riceve la conferma della ricezione da parte del Fornitore della propria accettazione.

⁶ In senso conforme V. SCORZA G., *Il contratto del commercio elettronico*, in CASSANO G., CIMINO P. I., *Diritto dell'internet e delle nuove tecnologie telematiche*, CEDAM, 2009, p. 168. Sul problema della "forma scritta" V. anche PERLINGIERI G., *op cit.*, pp. 293 ss., secondo cui il D.lgs 70/2003 non richiederebbe la forma scritta dell'informazione, cosa che avrebbe sollevato la questione della eventuale necessità della firma digitale; peraltro, secondo l'autore tale problema verrebbe comunque superato dall'efficacia formale estesa alle firme elettroniche deboli introdotte dal D.lgs 10/2002. La tesi dell'autore, sotto questo profilo, non merita di essere condivisa. Deve, infatti, rilevarsi che, attualmente, la materia è regolata dal D.lgs 82/2005 (come modificato dal D.lgs 235/2010) che ha conferito piena efficacia probatoria alle firme elettroniche qualificate,



Dott. Roberto Alma

Ciò premesso sulla concreta funzione della *ricevuta* prevista dal cit. art. 13 del D.lgs 70/2003, occorre, pertanto, comprendere quale sia la reale efficacia probatoria della medesima, avendo cura di sottolineare come nella maggior parte dei casi questa rivestirà la forma di un messaggio di posta elettronica (non certificata).

A tal riguardo, appare doveroso richiamare la disciplina normativa dettata in materia di *documento informatico* e oggi contenuta negli artt. 20 ss. del Decreto Legislativo 7 marzo 2005, n. 82 “Codice dell’Amministrazione Digitale”, (d’ora, innanzi, per brevità “C.A.D”), come modificato dal D.lgs 235/2010.

In particolare, rileva sul punto l’art. 21 del C.A.D che, infatti, precisa che il *documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.*

Ne deriva, pertanto, che la risposta al suddetto interrogativo non potrà prescindere dall’analisi delle numerose pronunce della giurisprudenza di merito che, in casi analoghi, si sono interrogate sul valore probatorio dei messaggi di posta elettronica.

A tal riguardo, si segnala l’esistenza di due orientamenti contrapposti:

- i) secondo un primo orientamento (più risalente) una dichiarazione trasmessa per posta elettronica costituirebbe prova scritta a tutti gli effetti di legge, in quanto considerata alla stregua di un documento sottoscritto con firma elettronica *semplice*, posto che il mittente, per poter creare ed inviare detta mail, dovrebbe, infatti, eseguire un’operazione di validazione, inserendo il proprio username e la propria password

digitali ovvero avanzate.



Dott. Roberto Alma

(Trib. Cuneo 15-12-2003⁷; Trib. Verona 26-11-2005⁸; Trib. Cassino 24-02-2009⁹);

- ii) secondo un diverso (e più recente) orientamento, il messaggio di posta elettronica non sarebbe, invece, idoneo ad integrare un documento informatico dotato di firma elettronica semplice, tenuto conto che non potrebbe ravvisarsi, in tale ipotesi, la connessione logica tra i dati validanti (User e Password) e il contenuto del singolo messaggio da validare (Trib. Roma 27-05-2010¹⁰, nello stesso senso V. anche Trib. Prato 15-04-2011¹¹, Trib. Brescia 11-03-2008¹²; T.A.R. Calabria 9 Febbraio 2005 n. 98¹³).

Ne deriva, pertanto, che alla luce del contrasto giurisprudenziale sopra riportato, il

⁷ Il *leading case* in materia è la sentenza del Tribunale di Cuneo del 15-12-2003, con nota di PANI M., *Il valore di prova scritta di una e-mail: la giustizia inizia a porsi al passo con i tempi*, in Giur. Merito, 2005. In particolare, si evidenzia che il procedimento di validazione costituito dall'inserimento dell'username e della password è stato considerato equivalente ad una firma elettronica leggera, tenuto conto del fatto che la definizione contenuta nell'art. 1 comma 1, lett. c) D.P.R. n. 445 del 2000 per firma elettronica si deve intendere *l'insieme dei dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati quale metodo di autenticazione informatica*. Sul punto, l'autore cita, altresì, la Delibera del CNIPA con la quale era stato ammesso che un sistema di autenticazione basato su User ID e Password fosse effettivamente idoneo giuridicamente a generare una firma elettronica leggera e, quindi, in grado di attribuire valore di forma scritta al documento informatico di riferimento. Nello stesso senso V. Trib. Bari 20-01-2004; Trib. Lucca, Sez. Lav., 17-07-2004; Trib. Mondovì, 7-06-2004.

⁸ **Trib. Verona 26-11-2005**, secondo cui *L'e-mail contenente una promessa di pagamento costituisce prova scritta anche ai fini della pronuncia del decreto ingiuntivo, poiché, essendo un documento informatico, la presenza di un codice identificativo permette d'individuare la sua provenienza ed, inoltre, si può equiparare al telegramma non accompagnato da un originale sottoscritto valutato come scrittura privata in base all'art. 2705 c.c.*

⁹ **Trib. Cassino 24-02-2009**: *Al fine di stabilire se la e-mail possa costituire prova scritta non solo idonea a consentire l'emissione del decreto ingiuntivo, questione che è stata oramai risolta in senso positivo, ma pure prova scritta idonea a fornire la prova del credito in sede di cognizione ordinaria, dovendo individuare quale sia l'efficacia probatoria delle e-mail non certificate, si rende necessario chiarire quale sia il ruolo del provider nel processo di elaborazione della posta elettronica. E' noto, da un lato, che tutti i providers predispongono registri elettronici, detti logs, in cui vengono salvati tutti i messaggi di posta elettronica in entrata ed in uscita relativi ad ogni utente (al fine precipuo di prevenire contestazioni), e, dall'altro, che tali soggetti devono avvalersi di specifici softwares che consentono di recuperare tutti i messaggi di posta elettronica di ogni singolo utente, anche se cancellati. Questo sistema consente al giudice, in caso di controversia sulla provenienza del messaggio di posta elettronica, di richiedere a ben due soggetti (il provider di invio ed il provider di ricezione del messaggio di posta elettronica) di fornire la controprova dell'avvenuto scambio della e-mail, atteso che del messaggio in partenza e di quello in arrivo è sempre conservata traccia nei computers dei providers. Ciò rende dunque possibile stabilire con sufficiente certezza se il messaggio di posta elettronica sia stato effettivamente inviato da un indirizzo di posta elettronica abilitato su un determinato provider ad un altro indirizzo di posta elettronica del pari "autenticato" su altro determinato provider. Da quanto esposto consegue che il messaggio di posta elettronica costituisce prova della sua provenienza e delle dichiarazioni in esso contenute, salvo che non sorga contestazione sulla sua autenticità e sulla sua effettiva spedizione/ricezione. In tal caso, la parte interessata (o il giudice ex officio) potranno acquisire informazioni presso i providers al fine di verificare la fondatezza della contestazione.*



Dott. Roberto Alma

consumatore potrebbe (com'è stato autorevolmente sostenuto) incorrere nel concreto rischio di non essere in grado di azionare efficacemente i propri diritti nei confronti del Fornitore laddove l'eventuale organo giudicante dovesse affermare l'irrelevanza probatoria del messaggio di posta elettronica contenente le informazioni prescritte dal cit. art. 13 D.lgs 70/2003¹⁴, (non potendo il consumatore, peraltro, neppure vantare alcun legittimo affidamento sul contenuto stesso dell'accordo che, infatti, potrebbe essere *medio tempore* modificato dal Fornitore).

Da questo punto di vista, la soluzione tecnica offerta da Elaborazioni Digitali s.r.l., offre, a ragion veduta, una maggior tutela al consumatore, in quanto - all'esito del procedimento tecnico brevettato in cui si sostanzia il Servizio *de quo*¹⁵ - l'Utente potrà ricevere, attraverso

¹⁰ V. Trib. Roma 12-5-2010, con nota di BARBARO S., *Un decreto ingiuntivo fondato sulla produzione di una mail: la posta elettronica non certificata non supera il vaglio del Tribunale di Roma*, in Riv. Dir. Inf., 2010, in cui il Giudice ha disconosciuto qualunque valore probatorio delle email prodotte in atti ritenendo che il dispositivo di riconoscimento tramite password per l'accesso alla posta elettronica semplice ovvero non certificata non avesse alcuna caratteristica oggettiva di qualità, sicurezza, integrità ed immodificabilità, e dunque garanzia di attendibilità.

¹¹ Trib. Prato 15-04-2011: *L'e-mail, quale documento informatico munito di firma semplice, non assicura di per sé né il contenuto né la provenienza del messaggio: è, pertanto, liberamente valutabile dal giudice, il cui giudizio, ai fini della qualificazione probatoria, dovrà fondarsi anche su altre risultanze processuali.*

¹² Trib. Brescia 11-03-2008: *Il messaggio di posta elettronica non certificato ai sensi del D.P.R. 11 febbraio 2005, n. 68 e privo di firma digitale a crittografia asimmetrica ai sensi del D.Lgs. 7 marzo 2005, n. 82 non può fornire alcuna certezza circa la propria provenienza o sull'identità dell'apparente sottoscrittore, così che esso non può venire qualificato alla stregua di un atto pubblico.*

¹³ T.A.R. Calabria Catanzaro Sent., 09/02/2005, n. 98: *Il ricorso gerarchico inoltrato per mezzo della posta elettronica, sebbene si intenda inviato e pervenuto all'amministrazione destinataria in quanto trasmesso all'indirizzo elettronico da questa dichiarato, non soddisfa il requisito legale della forma scritta se ad esso non è apposta una firma digitale o altro tipo di firma elettronica avanzata. Pertanto, da un lato, la detta trasmissione telematica non può considerarsi equipollente alla trasmissione a mezzo posta ordinaria, dall'altro, il ricorso gerarchico in tal modo inoltrato deve considerarsi irrituale.*

¹⁴ SCORZA G., *Il contratto del commercio elettronico*, in CASSANO G., CIMINO P. I., *Diritto dell'internet e delle nuove tecnologie telematiche*, CEDAM, 2009, p. 159.

¹⁵ Più precisamente, il procedimento prevede: **a)** la trasmissione elettronica degli estremi del contenuto dell'accordo definito e raggiunto tra il Fornitore/Preponente e l'Utente, il quale indicherà a NotarOK (Elaborazioni Digitali s.r.l.) il proprio numero di telefonia mobile, nonché il proprio indirizzo di posta elettronica (ove possibile certificata); **b)** il successivo invio da parte di NotarOK (Elaborazioni Digitali S.r.l.) di un messaggio SMS indirizzato all'Utenza precedentemente indicata contenente un codice univoco ed un collegamento ipertestuale (quest'ultimo inviato anche al sopra indicato indirizzo di posta elettronica); **c)** l'apertura da parte dell'Utente della pagina web richiamata dal collegamento ipertestuale sopra indicato (entro un intervallo di tempo predeterminato e attraverso un unico tentativo di utilizzo) contenente il contenuto del regolamento contrattuale *de quo*; **d)** l'apposizione da parte dell'Utente, previa lettura del predetto contenuto, del



Dott. Roberto Alma

un messaggio di posta elettronica certificata, la *ricevuta* prevista dall'art. 13 cit., (in forma di documento informatico firmato digitalmente e provvisto di una marcatura temporale, con esatta indicazione degli estremi temporali di ogni fase della procedura, nonché degli indirizzi IP utilizzati da entrambe le parti) che sarà idonea, a tutti gli effetti di legge, a provare sia l'esistenza del contratto sia il relativo contenuto (così come concordato tra le parti).

A tal riguardo appare doveroso precisare che la ricevuta verrebbe ad essere sottoscritta digitalmente da NotarOK, in qualità di rappresentante "virtuale" (cd. *Software Agent*) del Fornitore¹⁶, ai sensi degli artt. 1387 ss. cc., con conseguente diretta imputabilità giuridica di tale documento al Fornitore medesimo.

Per quanto attiene alla validazione temporale si evidenzia che la stessa consentirà di attribuire data certa al documento in questione, ai sensi dell'art. 20 comma 3 del C.A.D., secondo cui l'apposizione della data e dell'ora di formazione del documento informatico è opponibile ai terzi¹⁷ purché ciò sia avvenuto in conformità delle regole tecniche emanate ai sensi dell'art. 71 C.A.D e attualmente contenute nel D.P.C.M 30-03-2009¹⁸.

Si segnala, inoltre, per mera completezza di esposizione, che l'art. 37 del cit. D.P.C.M, espressamente ribadisce che i riferimenti temporali realizzati dai certificatori accreditati in

codice univoco ricevuto via sms; e) la riproposizione da parte di NotarOK (Elaborazioni Digitali S.r.l.), previa verifica del codice univoco precedentemente apposto dall'Utente, di una seconda pagina web contenente l'indicazione delle clausole per le quali si richiede la specifica approvazione dell'Utente, mediante nuova immissione del codice univoco di cui sopra; f) l'informativa di NotarOK (Elaborazioni Digitali S.r.l.) inviata a mezzo messaggio di Posta Elettronica Certificata sia al Fornitore/Preponente sia all'Utente avente ad oggetto il buon esito del processo, con riproduzione del contenuto del contratto, indicazione dell'orario e dell'indirizzo IP utilizzato in ogni fase dalle parti; g) la memorizzazione dell'accordo così sottoscritto da parte di NotarOK (Elaborazioni Digitali S.r.l.) su supporto durevole immutabile con apposizione di firma digitale e marcatura temporale.

¹⁶ Sulla natura dei *Software agent*, V. BRAVO F., *Il contratto cibernetico*, Riv. Dir. Inf. 2011, pp. 170 ss., il quale definisce i *software agent* come applicativi che, sfruttando l'intelligenza artificiale, agiscono secondo schemi operativi che replicano, in senso lato, il modello della rappresentanza. In altre parole, secondo l'Autore, i programmi in questione agirebbero, sotto il profilo tecnico e socio-relazionale, come fossero dei rappresentanti dell'utente, stabilendo con un certo grado di autonomia se stipulare o meno il contratto. Nell'ipotesi di NotarOK, più precisamente, l'apposizione della firma digitale di quest'ultimo dipende unicamente dalla corretta ultimazione delle fasi in cui si articola il procedimento tecnico di sottoscrizione.

¹⁷ Ciò implica, ovviamente, che il documento regolarmente vidimato ex art. 20 comma 3 sarà pienamente efficace nei confronti dei terzi

¹⁸ Le suddette regole tecniche sono in vigore, quantomeno, sino all'approvazione delle nuove Regole Tecniche di cui alla Bozza di *Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni e di gestione del fascicolo informatico* del 5/08/2011.



Dott. Roberto Alma

conformità con quanto previsto negli artt. 43 ss. sono opponibili ai terzi ai sensi dell'art. 20, comma terzo del C.A.D, (come nel caso del Servizio esaminato nella fattispecie, poiché, la validazione temporale apposta da NotarOK è rilasciata da un certificatore accreditato)

Più precisamente, l'art. 43 del cit. D.P.C.M. prevede espressamente che la validazione temporale debba avvenire mediante generazione ed applicazione di una marca temporale¹⁹ alla relativa impronta dell'evidenza informatica da validare.

L'art. 47 dello stesso D.P.C.M poi precisa che il riferimento temporale assegnato ad una marca temporale deve coincidere con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al *decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591* (elementi, questi, tutti rinvenibili nella marcatura temporale apposta da NotarOK).

Alla luce di quanto sopra espresso sulla (indubbia) rilevanza di NotarOK per quanto attiene alla generazione di una *ricevuta* ex art. 13 D.lgs 70/2003 (provvista di piena efficacia formale e probatoria, nella quale si estrinseca la sua peculiare funzione di certificazione del contratto), si deve, a questo punto, procedere ad un'analisi sulla possibilità di utilizzare concretamente il procedimento brevettato²⁰ oggetto del Servizio onde consentire all'Utente di sottoscrivere validamente un documento informatico a tutti gli effetti di legge anche in assenza della titolarità di un dispositivo di firma digitale (In altre parole, occorre chiarire se ai fini del soddisfacimento del requisito della forma scritta *ad substantiam* ovvero della forma scritta *ad probationem* sia comunque necessariamente richiesto *ex lege* l'utilizzo della firma digitale - o di una firma elettronica qualificata - dell'interessato o se siano ammissibili ulteriori procedimenti di sottoscrizione elettronica).

La questione è di rilievo poiché, a titolo meramente esemplificativo, nei contratti che

¹⁹ La marca temporale, ex art. 43, II° comma, del D.P.C.M. 30/03/2009, è generata da un apposito sistema di validazione temporale, sottoposto ad opportune personalizzazioni atte a innalzarne il livello di sicurezza, in grado di: a) garantire l'esattezza del riferimento temporale conformemente a quanto richiesto dal presente decreto; b) generare la struttura dei dati temporali secondo quanto specificato negli *articoli 44 e 47* del presente decreto; c) sottoscrivere digitalmente la struttura di dati di cui alla lettera b). L'art. 44 stabilisce, invece, il contenuto obbligatorio della marca temporale, ovvero: a) identificativo dell'emittente; b) numero di serie della marca temporale; c) algoritmo di sottoscrizione della marca temporale; d) identificativo del certificato relativo alla chiave di verifica della marca temporale; e) riferimento temporale della generazione della marca temporale; f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale; g) valore dell'impronta dell'evidenza informatica.

²⁰ Il riferimento è alla domanda di brevetto nazionale N. MI2010A000184 depositata in data 8 febbraio 2010, avente titolo *Sistema e metodo per la stipulazione di contratti*.



Dott. Roberto Alma

ricadono sotto l'alveo applicativo degli artt. 1341, 1342 cod. civ, ovvero degli artt. 33 ss. del D.lgs 206/2005, determinate clausole necessitano, ai fini della loro efficacia, di specifica approvazione scritta.

Sul punto rileva l'art. 20 comma 1-bis del C.A.D., secondo cui, per quanto qui interessa, *l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.*

Gli unici casi in cui, quindi, la firma digitale o qualificata è espressamente richiesta a pena di nullità concernono, oggi, **esclusivamente** gli atti previsti dall'art. 1350 c.c., nn. 1-12²¹, secondo quanto espressamente disposto dal novellato art. 21 comma 2-bis del C.A.D²² che, pertanto, costituisce norma *speciale* rispetto alla norma *generale* di cui all'art. 20 comma 1-bis, con conseguente inammissibilità dell'applicazione analogica ai casi non espressamente previsti (quali, per l'appunto, a titolo meramente esemplificativo, l'approvazione specifica delle clausole di cui all'art. 1341 comma secondo).

Di conseguenza, il giudice investito della questione della rilevanza formale del documento informatico, (privo di firma ovvero sottoscritto con qualsivoglia firma elettronica), può liberamente valutarlo²³, (tenuto conto dei parametri indicati dallo stesso C.A.D che verranno più diffusamente esaminati in seguito).

Per quanto, invece, attiene al valore probatorio del documento informatico sottoscritto con firme elettroniche diverse da quella digitale o qualificata, rileva l'art. 21 del C.A.D che -nella

²¹ V. sul punto SANTACROCE B., *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei dispositivi di firma*, SIAV ACADEMY, 2011, p. 2, in quale rileva che *solamente per gli atti di costituzione e trasferimento dei diritti reali immobiliari di cui all'articolo 1350 del codice civile viene richiesta obbligatoriamente la sottoscrizione, a pena di nullità, con firma qualificata o digitale.*

²² Giova precisare che il Decreto Legislativo n. 235 del 2010 ha inserito l'art. 21 comma 2-bis, abrogando, al contempo, l'art. 20 comma 2 che testualmente prevedeva che *il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.*

²³ V. BARBARO S., *op cit.*, il quale ha evidenziato come nella previgente disciplina dettata dal C.A.D. in materia di documento informatico il riconoscimento dell'efficacia della forma scritta spettasse unicamente ai documenti sottoscritti con firma digitale o con firma elettronica qualificata.



Dott. Roberto Alma

sua formulazione vigente - stabilisce che:

a) Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità;

b) Il documento informatico sottoscritto con firma elettronica **avanzata** (ma anche **digitale** o **qualificata**) formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile.

A tal riguardo, per comprendere appieno l'efficacia probatoria del procedimento di sottoscrizione del contratto offerto da NotarOK attraverso il Servizio *de quo*, sarà opportuno evidenziarne le caratteristiche di qualità, sicurezza, integrità e immodificabilità, per poi verificare se sia invocabile la disciplina prevista per il documento informatico con firma elettronica semplice ovvero con firma elettronica avanzata.

Alla luce dell'analisi della documentazione tecnica inerente al Servizio qui esaminato emerge che lo stesso risulta soddisfare pienamente i parametri tecnici sopra menzionati, poiché:

- il codice PIN utilizzato dal consumatore per *firmare* il contratto è unico per ogni transazione/utente ed è inviato mediante connessioni sicure - come *Short Message Service* - esclusivamente ad un utenza telefonica indicata dallo stesso (della quale si presume che abbia la disponibilità esclusiva) purché relativa ad una SIM/USIM rilasciata all'Utente rispettando le disposizioni dettate dall'art. 55 del D.lgs 259/03²⁴. Ciò garantisce il fondamentale requisito della *sicurezza*, quello della *connessione univoca* dei dati utilizzati per la validazione del documento al firmatario (superando così le perplessità della giurisprudenza in merito all'utilizzo di PIN²⁵), nonché quello dell'*identificazione certa* del firmatario, in ottemperanza alle prescrizioni del Ministero dell'interno contenute nella nota datata 5 novembre 2007²⁶;

²⁴ La suddetta disposizione prevede l'identificazione completa dell'utente prima dell'attivazione del servizio.

²⁵ V. Trib. Roma 27 – 05 – 2010, in cui si è rilevato che nel caso delle email, l'utilizzo di un sistema di autenticazione composto da User ID, password (o codice PIN), non vale, in assenza di altri strumenti tecnici, a garantire la validazione dei dati che costituiscono il messaggio di posta elettronica.

²⁶ Il Ministero dell'Interno ha, infatti, ritenuto che, con riferimento all'identificazione dell'Utente che si connette alle reti di comunicazione elettronica attraverso la tecnologia Wireless, costituisce condizione sufficiente per soddisfare i requisiti previsti dalla normativa vigente l'utilizzo del telefono mobile quale mezzo per attivare le procedure necessarie ad ottenere le credenziali di accesso alla rete stessa consentendo



Dott. Roberto Alma

- l'apposizione, in via del tutto automatica, della firma digitale da parte di NotarOK alla ricezione dell'impulso elettronico da parte dell'Utente sul documento in questione assolve, inoltre, alla funzione di garantire l'immodificabilità e l'integrità dello stesso, trattandosi di una firma elettronica rilasciata da un certificatore accreditato, nonché conforme alle regole tecniche contenute nel vigente D.P.C.M 30 marzo 2009 in materia di firme elettroniche digitali.

Di conseguenza, anche riconducendo il documento informatico così sottoscritto alle previsioni di cui all'art. 21 comma 1 lett. a), non sembra, tuttavia, revocabile in dubbio la rilevanza formale e/o probatoria del medesimo.

In ogni caso, le peculiarità del Servizio qui esaminato inducono, altresì, a ricondurre la procedura di sottoscrizione del relativo documento informatico alla disciplina prevista in materia di apposizione di firme elettroniche avanzate, la cui definizione è stata introdotta nel C.A.D. dall'art. 1 comma 1 lett. e) del D.lgs 235 del 2010 che ha, infatti, aggiunto una lettera q-bis all'art. 1 comma 1 del C.A.D. che, per l'appunto, definisce la firma elettronica avanzata come *l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*²⁷.

l'identificazione, seppur indiretta, dell'interessato.

²⁷ La firma elettronica avanzata, come si è già accennato sopra, non era originariamente menzionata nell'originaria formulazione degli artt. 20 e 21 del C.A.D., i quali erano ancorati alla tripartizione tra firma elettronica semplice, firma elettronica qualificata e firma digitale, con ciò differenziandosi dalle previsioni della Direttiva 1993/93/CEE, relativa ad un quadro comunitario per le firme elettroniche, che si limitava, invero, a distinguere tra firma elettronica semplice e firma elettronica avanzata. Infatti, secondo il previgente art. 1 del C.A.D., si doveva intendere per: a) **firma elettronica**: *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica*; b) **firma elettronica qualificata**: *la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, 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 sono stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica*; c) **firma digitale**: *un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*. Sul punto si veda l'ampia analisi di DUNI G., *Le firme elettroniche nel diritto vigente (Osservazioni sulla normativa italiana nel 2006)*, in Riv. Dir. Inf., 2006, pp. 505 ss., in cui si evidenzia che, nell'impianto del Codice dell'Amministrazione Digitale emanato nel 2005, la cd. "firma elettronica avanzata", prevista dalla Direttiva 93/1993/CE, dovrebbe rientrare all'interno della definizione di



Dott. Roberto Alma

La definizione di firma elettronica avanzata di cui al cit. art. 21 del C.A.D. riprende, comunque, senza sostanziali modificazioni, la definizione contenuta nell'art. 2.2 della Direttiva 93/1993/CE in materia di firme elettroniche²⁸.

A questo punto, occorre domandarsi se la procedura di sottoscrizione del contratto compiuta attraverso il Servizio NotarOK possa integrare o meno l'apposizione di una firma elettronica avanzata - che secondo l'orientamento prevalente in dottrina dovrebbe ricomprendere tutte le ipotesi di firme elettroniche con tecnologie RSA²⁹ - stante la natura *aperta* della definizione contenuta nella citata Direttiva Europea³⁰ (e ferma restando, in ogni caso, la necessità di attendere la definitiva approvazione delle nuove regole tecniche in

firma elettronica contenuta nell'art. 1 lett. q), pur essendo oggettivamente ad un livello tecnologicamente superiore. Al riguardo, per mera completezza di esposizione preme qui precisare che la firma elettronica avanzata era, in realtà, stata introdotta nell'ordinamento italiano con il D.Lgs n. 10 del 2002 e con il D.P.R. n. 137 del 2003; cfr., in particolare, l'analisi condotta sul punto da IZZI B., *La firma elettronica negli strumenti di circolazione della ricchezza*, in Riv. Dir. Notariato, 2004, pp. 867 ss., in cui si evidenzia che nell'assetto così realizzato, la firma digitale viene ad essere ricondotto all'interno delle cd. firme forti o avanzate. Più precisamente l'art. 6 del cit. D.lgs 10/2002 ha modificato l'art. 6 del T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, approvato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, prevedendo che il documento informatico sottoscritto con firma elettronica soddisfa il requisito della forma scritta e che quando è sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione della firma sicura, fa inoltre piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritto. L'Autore, tuttavia, rileva giustamente la sussistenza di una disciplina parzialmente contraddittoria poiché l'art. 11 del D.P.R. n. 445 del 2000, come modificato dal D.P.R. n. 137 del 2003, nel disciplinare la rilevanza dei contratti stipulati con strumenti telematici ed informatici faceva riferimento alla firma elettronica qualificata e non alla firma elettronica avanzata, la quale, secondo l'art. 1, lett. ee) del D.P.R. 445/2000 (anch'esso modificato dal D.P.R. n. 137 del 2003) era definita come un sotto-tipo di firma avanzata.

²⁸ La richiamata disposizione di cui all'art. 2.2 definisce, infatti, la firma elettronica avanzata come una firma elettronica che soddisfi i seguenti requisiti: *a) essere connessa in maniera unica al firmatario; b) essere idonea ad identificare il firmatario; c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo; d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;*

²⁹ Sulle firme RSA V. RIVEST, SHAMIR, ADLEMAN, *A method for obtaining Digital signature and public key cryptosystems*, in Communications of the Acm, vol. 21, pp. 120-126. Sulla equiparazione tra firma elettronica avanzata e firme RSA V. DUNI G., *op. cit.*, pp. 505, il quale ritiene che le firme avanzate sarebbero basate sullo stesso metodo RSA (criptazione asimmetrica) delle firme digitali ma, in quanto prive di certificato, giuridicamente sarebbero mere firme elettroniche..

³⁰ V. BORRUSO R., *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (d.lgs 23 gennaio 2002 n. 10, d. p. r. 7 aprile 2003 n. 137 e l. 29 luglio n. 229)*, in Giust. Civ., 2004, 3, pp. 153 ss., il quale ha, invero, rilevato che *il legislatore europeo ha previsto un sistema computerizzato di autenticazione degli scritti sostitutivo della sottoscrizione autografa più largo di quello realizzato con la firma digitale nel senso che, fermo restando quest'ultimo sistema in tutti i suoi dettagli già normativamente precisati, esso possa essere affiancato da altri sistemi di efficacia giuridica perché di pari affidabilità tecnica.* V., altresì,



Dott. Roberto Alma

materia di firme elettroniche attualmente in stato di consultazione pubblica³¹).

Si rileva a tal riguardo che:

- i) l'**identificazione** del firmatario verrebbe integrata dalla duplice identificazione via email e, soprattutto, *sms*, secondo quanto già illustrato in precedenza;
- ii) la **possibilità di attribuire il documento in maniera univoca** al firmatario verrebbe garantita, come già accennato, dall'invio di un codice alfanumerico unico per ogni transazione e dalla limitata validità temporale³² su un utenza telefonica nella esclusiva disponibilità del consumatore/utente ed appartenente all'arco di numerazione italiano;
- iii) il **controllo esclusivo** del firmatario del sistema di generazione della firma deriverebbe dalla totale automaticità della procedura che, in ogni caso, presuppone specifici impulsi volitivi del firmatario inviati in via elettronica;
- iv) l'**immodificabilità** del documento così sottoscritto sarebbe, invece, garantita dall'immediata apposizione, in via automatica, della firma digitale di NotarOK (a tutti gli

DELFINI F., *Documento informatico e firme elettroniche*, in VALENTINO D., (a cura di), *Manuale di Diritto dell'informatica*, Napoli, Edizioni Scientifiche Italiane, seconda edizione, **2011**, pp. 515-516, in cui si evidenzia che l'approccio adottato dal legislatore comunitario è stato tecnologicamente neutro, con un allargamento dei concetti: non firma *digitale*, che richiama un preciso standard tecnologico, ma firme *elettroniche*, con riguardo alle funzioni da esse svolte.

³¹ Sul punto V. SANTACROCE B., *op cit* p. 4, il quale ritiene che, dalla lettura della bozza di regole tecniche del 4 luglio 2011, emergerebbe che la soluzione di firma avanzata per essere valida ed in linea con le regole tecniche stesse dovrebbe garantire l'identificazione del firmatario del documento, la connessione univoca della firma al firmatario stesso ed il controllo esclusivo di questo sul sistema di generazione della firma.

³² Ciò consentirebbe, ad avviso di chi scrive, il superamento delle ben note perplessità della dottrina in merito all'utilizzo di *password* e/o PIN, per cui V., in particolare, BORRUSO R., *op. cit.*, pp. 155 ss., che ritiene "opportuna" la qualificazione di *firma elettronica debole* da attribuire ai predetti strumenti di sottoscrizione, sia per la loro scarsa segretezza, sia per la possibilità di essere abusivamente clonati attraverso l'uso di elaboratori anche di media potenza. Nel caso di NotarOK, invece, il PIN viene inviato, come già anticipato, attraverso connessioni sicure esclusivamente all'utenza telefonica indicata dall'Utente ed è unico per ognuno di essi. In senso conforme V. FINOCCHIARO G., *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, Contratto e Impresa, 2011, p. 498, la quale ritiene che, a titolo esemplificativo, la *one-time-password* utilizzata da alcune banche (analoga al codice PIN inviato da NotarOK) costuisca, a tutti gli effetti, un'ipotesi di firma elettronica avanzata.



Dott. Roberto Alma

effetti, una *firma digitale di sistema*³³), produttiva degli effetti previsti dall'art. 21 del C.A.D.³⁴.

Tutto ciò considerato, si deve, comunque, concludere che, a prescindere dalla qualificazione del suddetto procedimento di sottoscrizione come apposizione di una firma elettronica **semplice** o **avanzata**, non sembra revocabile in dubbio che il documento informatico così sottoscritto sia, in virtù delle particolari caratteristiche tecniche del Servizio (ampiamente illustrate), valido ed efficace a tutti gli effetti di legge, rispettando tutti i requisiti specifici previsti dagli artt. 20 e 21 del C.A.D.

Rimango a disposizione per chiarimenti ed attendo Vostre in merito a quanto sopra espresso.

Cordialmente

Roberto Alma

³³ V. DUNI G., *op. cit.*, p. 510, il quale evidenzia che il criterio dell'*immodificabilità* può ottenersi o creando un documento con la tecnologia RSA, anche non qualificata, oppure conservando il documento su supporto WORM, ovvero ancora applicando una firma digitale di sistema al momento della ricezione, possibilmente in modo automatizzato. In particolare l'Autore, con riferimento alla P.A., sostiene che *se il messaggio di ricevuta fosse munito di firma digitale e riproducesse anche il testo del messaggio del cittadino, la garanzia reciproca sarebbe massima: avremmo in tal modo semplificato le attività del cittadino, esentandolo dal munirsi della firma digitale;*

³⁴ Per completezza di esposizione, si rileva che la suddetta ricostruzione appare, in ogni caso, conforme all'attuale bozza di nuove regole tecniche in materia di firme elettroniche, atteso che il relativo art. 56, "caratteristiche delle soluzioni di firma elettronica avanzata", dispone che: *Le soluzioni di firma elettronica avanzata devono garantire: a) l'identificazione del firmatario del documento; b) la connessione univoca della firma al firmatario; c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma; d) la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma; e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto; f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a); g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati. La firma elettronica avanzata generata in violazione di quanto disposto da una o più disposizioni di cui alle lettere a), b), c), d), g) del comma precedente, non soddisfa i requisiti previsti dall'art.21, comma 2, del codice.*