Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea Magistrale in Scienze di Internet

Il domicilio digitale può facilitare l'interazione tra il cittadino e la p.a.?

Relatore: Chiar.mo
Prof.ssa Giusella
Finocchiaro

Presentata da:
Marilena Mordenti

Sessione I
Anno Accademico 2013/2014

Vorrei esprimere la mia profonda gratitudine alla Prof.ssa Giusella Finocchiaro per la sua grande disponibilità.

Un ringraziamento particolare alla Dott.ssa Annarita Ricci per il suo aiuto e la sua franchezza.

Un grazie speciale per avermi tollerato e sostenuto lungo questo percorso ad Anna Rosa, Brunella e Francesca.

Un ultimo grazie ad Eralda che mi è sempre stata vicino.

Ad Annalena e Simone

INDICE

“Che so bisognerebbe trovare qualcuno a cui chiedere
l’indirizzo di questa Marisa Florian“
“Domandiamo a quel militare là”
…
“Ma per andare dove dobbiamo andare
dove dobbiamo andare?”

(Totò Peppino e la… malafemmena, 1956)

Introduzione

La Legge di conversione n. 221/2012 del Decreto Legge n. 79/2012 *(*c.d. *Decreto Crescita 2.0)* introduce nel Codice dell’Amministrazione Digitale la facoltà per ogni cittadino di indicare alla pubblica amministrazione un proprio indirizzo di posta elettronica certificata quale suo domicilio digitale. La Legge di conversione n. 98/2013 del Decreto Legge n. 69/2013 *(*c.d. *Decreto del Fare)* prevede l’assegnazione di una casella di posta elettronica certificata, con funzione di domicilio digitale, contestualmente al rilascio del Documento Digitale Unificato al cittadino.

La disponibilità del domicilio digitale, costituito da una casella di posta elettronica certificata, può consentire alle amministrazioni pubbliche di dematerializzare le comunicazioni verso il cittadino indirizzandole al domicilio digitale con notevoli risparmi dovuti all’eliminazione della carta e delle spese spedizione.

In questo studio, *attorno* al domicilio digitale e alle comunicazioni via posta elettronica certificata, si cercherà di comprendere *come* e *con quali effetti*, il diritto di ogni cittadino di disporre di un domicilio digitale possa proficuamente essere esercitato nelle comunicazioni e nelle trasmissioni di documenti con la pubblica amministrazione.

Nel primo capitolo si procederà all'analisi delle disposizioni in materia di trasmissione di documenti informatici, individuate nel quadro normativo che si è venuto via via a creare sin dall'attribuzione di valore giuridico al documento informatico. Nel successivo capitolo si analizzerà la diversa valenza giuridica delle trasmissioni via posta elettronica ordinaria e certificata verificandone gli aspetti tecnici. Nel terzo si tratterà specificatamente del domicilio digitale e delle diverse tipologie di caselle di posta elettronica certificata presenti nel nostro Paese e della loro interoperabilità. Nel quarto si analizzeranno le problematiche relative alla tutela dei dati personali legati alla posta elettronica e ai reati penali in materia di violazione della corrispondenza. Nel quinto capitolo si cercherà di *ampliare la visione* individuando quali siano i diritti dei cittadini all'uso delle tecnologie e il reale esercizio.

Con le conoscenze acquisite si cercherà di dare una risposta al quesito all'origine di questo studio.

1. Dal domicilio tradizionale al domicilio digitale

In questo capitolo si tratterà innanzitutto della normativa dell'istituto giuridico del domicilio inteso come un luogo, nella sua dimensione fisica e spaziale. Si procederà quindi all'analisi di quelle leggi e quelle direttive che si sono succedute nel tempo in materia di informatizzazione della trasmissione documentale: ci si riferisce alla attribuzione di validità giuridica alle comunicazioni via e-mail e delle trasmissioni di documenti informatici intesi come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Si tratteranno le disposizioni in materia di posta elettronica e di posta elettronica certificata, fino ad arrivare alla normativa più recente che consente ad un soggetto (ed in alcuni casi *obbliga*) l'elezione di un proprio domicilio digitale, cioè di un indirizzo di posta elettronica certificata che va a costituire la sede principale virtuale dei suoi affari e interessi.

1.1 Il domicilio generale

La parola *diritto* si impiega in senso oggettivo per indicare le norme giuridiche, cioè le norme che prescrivono agli individui determinati comportamenti, ma la si impiega anche in senso soggettivo per indicare la pretesa di un soggetto che altri assumano il comportamento prescritto da una norma.

Ci sono diritti soggettivi che sono creati dal diritto oggettivo e invece diritti soggettivi che *si dicono solo 'trovati' dal diritto oggettivo* e sono i diritti spettanti all'uomo, sono cioè quei diritti che esistono indipendentemente da ogni norma giuridica che li riconosca, cosicché il diritto oggettivo si limita a garantirli. A differenza di ogni altro diritto soggettivo, la cui esistenza e mutevolezza dipende dai diversi decorsi storici dei sistemi politici o sociali, i diritti dell'uomo, detti anche diritti della persona umana o della personalità, si considerano spettanti all'uomo in quanto tale, ed ogni Stato ha il dovere di riconoscerli e garantirli. Sono il diritto alla vita, all'integrità fisica, alla salute, al nome, all'onore, alla libertà personale, all'espressione del pensiero, alla riservatezza e altri ancora, la cui identificazione è rimessa alle carte costituzionali e, in ambito

sovranazionale o internazionale, a convenzioni tra Stati, ratificate dagli Stati aderenti che ne hanno trasformato i contenuti in altrettante norme di diritto interno[(1)].

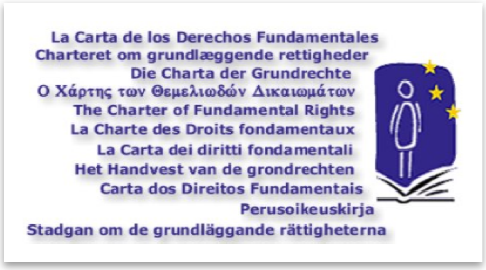
Ai diritti della personalità la Costituzione della Repubblica italiana fa riferimento all'art. 2: *"La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità"*, in questa materia non è applicabile alcuna riserva di legge in quanto, affinchè i diritti dell'uomo possano essere riconosciuti e garantiti, non occorre che una norma di legge li abbia previsti. Il loro carattere di inviolabilità, attribuito dall'art. 2 della Costituzione, ha un duplice significato: sono diritti dell'uomo inviolabili da parte della pubblica autorità nell'esercizio delle sue funzioni legislative, esecutive e giudiziarie; sono, inoltre, diritti dell'uomo inviolabili da parte di altri uomini nell'ambito dei rapporti tra privati. Sotto il primo aspetto sono da considerarsi le norme specifiche che, nella Costituzione, proclamano la libertà personale (art.13), l'inviolabilità del domicilio (art. 14), la libertà e segretezza nelle comunicazioni (art. 15), la libertà di circolazione (art. 16), la libertà di riunione (art. 17), la libertà di associazione (art. 18), la libertà di religione (art. 19), la libertà di manifestazione del pensiero e la libertà di stampa (art. 21), sotto il secondo aspetto assumono rilievo le norme che, nei codici o in altre leggi, tutelano i diritti inviolabili della persona nei confronti degli altri *consociati*. Proprio in questa prospettiva il codice penale sanziona i "delitti contro la persona" (art. 575 e ss. c.p.), distinguendoli in delitti "contro la vita e l'incolumità personale" (art. 575 e ss. c.p.) come l'omicidio, le percosse e le lesioni personali, "delitti contro l'onore" (art. 594 e ss. c.p.) come l'ingiuria e la diffamazione, "delitti contro la libertà individuale" (art. 600 e ss. c.p.) come la riduzione in schiavitù, il sequestro di persona, la violenza sessuale, la violenza privata, la violazione di domicilio. Il Codice Civile inoltre detta norme specifiche che riguardano il diritto all'integrità fisica (art. 5 c.c.), il diritto al nome (artt. 6-9 c.c.), il diritto sulla propria immagine (art. 10 c.c.), il diritto morale d'autore e di inventore (art. 2577 comma 2 e art. 2589).

---

(1) Rif: F.GALGANO, pagg. 148-149 in *[1]*

L’art. 2 della Costituzione riconosce e garantisce i diritti inviolabili dell’uomo nella sua globalità e non fa riferimento solo a quelli specificatamente tipizzati, bensì anche a quelli che la coscienza sociale in un determinato momento storico ritiene essenziali per la tutela della persona umana, in tal senso alcuni diritti della personalità sono detti *atipici* come ad esempio il diritto alla riservatezza e il diritto all’identità personale[(2)]. Si analizzerà ora in maniera più specifica il diritto della persona alla tutela del domicilio.

La Convenzione per la tutela dei diritti dell’uomo e delle libertà fondamentali[(3)] sancisce all’art. 8 che *“ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza”* e che *“non può esservi ingerenza di un’autorità pubblica nell’esercizio di tale diritto, a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell’ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui”*.



La Carta dei diritti fondamentali dell'Unione europea[(4)] dispone, all'art. 7, che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio, delle proprie comunicazioni.

---

(2) Rif: A.TORRENTE – P.SCHLESINGER, pagg. 123-124 in *[2]*

(3) La Convenzione per la tutela dei diritti umani e delle libertà fondamentali (Roma, 4 Novembre 1950) è entrata in vigore il 3 Settembre 1953. La Convenzione è stata istituita in seno al Consiglio d'Europa, un’organizzazione di cui fanno parte 47 paesi, per un ammontare complessivo di oltre 800 milioni di cittadini. Il Consiglio d’Europa rappresenta il più avanzato sistema di tutela dei diritti umani in campo internazionale, avendo istituito un organo pienamente giurisdizionale: la Corte Europea dei Diritti dell'Uomo, con sede a Strasburgo, con specifiche finalità di garanzia effettiva dei diritti da essa enunciati.

(4) La Carta dei diritti fondamentali dell'Unione europea è stata sottoscritta e proclamata dai Presidenti di Parlamento europeo, Consiglio e Commissione in occasione del Consiglio europeo di Nizza il 7 dicembre 2000. (Rif: *http://www.europarl.europa.eu/charter/default_it.htm*)

L’art. 14 comma 1 della Costituzione dispone: *“il domicilio è inviolabile”* a tutela della proiezione spaziale della persona, cioè del luogo o dei luoghi che rappresentano la sfera privata, che costituisce espressione della propria libertà individuale; al comma 2 sono previste garanzie in relazione alle limitazioni della libertà di domicilio, garanzie che tuttavia sono ridotte rispetto a quelle previste per la tutela della libertà personale (di cui all’art. 13) in quanto il comma 3, sempre dell’art. 14 dispone: *“Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali*”, questo a significare che non viene posta la riserva di legge giurisdizionale, in quanto il legislatore consente all’autorità amministrativa la possibilità di svolgere accertamenti all’interno del domicilio[(5)].

Il luogo in cui la persona fisica svolge la propria attività assume, per l’ordinamento giuridico, rilevanza sotto diversi punti di vista, specie in ambito *processuale* (ad esempio per la determinazione della competenza territoriale, come da art. 18 del Codice di Procedura Civile, in merito al Foro generale delle persone fisiche, del luogo di notificazione, come da art. 139 e ss. sempre del c.p.c.) ma anche in ambito *sostanziale* (ad es. l’art. 456 c.c. dispone che la successione si apre nel luogo dell’ultimo domicilio del defunto, l’art. 1182 c.c. statuisce che l’obbligazione, avente per oggetto una somma di danaro, deve essere adempiuta al domicilio del creditore al tempo della scadenza e che negli altri casi l’obbligazione deve essere adempiuta al domicilio che il debitore ha al tempo della scadenza, ecc.).

Nel libro primo del Codice Civile, l’art. 43, comma 1, regolamenta il domicilio definito come il luogo in cui una persona *“ha stabilito la sede principale dei suoi affari e interessi”*. I punti salienti della disposizione sono due: l’oggettiva prevalenza di una sede di *affari ed interessi* e secondo, gli *interessi* non sono solo di natura economica, ma anche personale, sociale, politica: per esempio, se gli affari professionali di un individuo si dividono tra Milano e Roma ma egli vive con la famiglia a Milano, prevarrà quest’ultima sede[(6)]. .

---

(5) Rif: A.TORRENTE – P.SCHLESINGER, pagg. 116-117 in *[2]*

(6) Rif: S.PANIZZA – E.STRADELLA, pagg. 361-362 in *[3]*

Quanto sino ad ora esplicitato è il *domicilio generale* che coincide normalmente, ma non necessariamente, con la residenza che *è nel luogo in cui la persona ha la dimora abituale*, in quanto è possibile svolgere la propria attività professionale in un Comune, avendo in quel Comune il domicilio, ed abitare in un altro, avendo in quest'ultimo la residenza. Il significato del termine *dimora* è quello consueto: il luogo in cui una persona si trova ad abitare. Occorre tuttavia un minimo di stabilità: se il soggetto si sposta per affari, egli non cambia dimora ogni sera; se invece va un mese in vacanza, allora cambia dimora. Si può avere più di una *residenza di fatto*, ed è il caso ad esempio, in cui una persona dimori sei mesi in città e sei mesi in campagna[(7)].

La residenza è un fatto giuridico ed è oggetto di pubblicità nei registri anagrafici. Se una persona cambia residenza e non *"denuncia il fatto nei modi previsti dalla legge"*, come dispone l'art. 44 c.c., il cambiamento non è opponibile ai terzi in buona fede. Non è prevista, al contrario, nessuna registrazione pubblica del domicilio; se richiesta una attestazione di domicilio, la stessa può essere effettuata attraverso una dichiarazione sostitutiva di atto di notorietà ma solo dai cittadini italiani e comunitari. Non possono dichiarare il domicilio i cittadini extracomunitari in quanto si tratta di dato non attestabile o certificabile da soggetti pubblici italiani (art. 3 comma 2 del D.P.R. 445/2000). Per le persone giuridiche l'art. 46 c.c. dispone che, quando la legge fa dipendere determinati effetti dalla residenza o dal domicilio, si ha riguardo al luogo in cui è stabilita la sede.

Il domicilio costituisce dunque un elemento fondamentale nella determinazione e nella regolamentazione della relazione giuridica della persona con il territorio: il soggetto che stabilisce il proprio domicilio in un determinato luogo, infatti, sa che la legge presume che si trovi in quel luogo. Per gli effetti che la legge lega alla individuazione della persona sul territorio, ogni individuo ha un unico *domicilio generale* (di cui all'art. 43 c.c.).

---

(7) Rif: G.IUDICA – P.ZATTI, pagg. 89-90 in *[4]*

1.2 Le altre tipologie di domicilio

Dal domicilio generale si distingue il *domicilio speciale* o *elettivo*: in questo caso è essenziale la dichiarazione del soggetto che elegge domicilio in una sede per determinati atti o affari (art. 47 c.c.) come ad esempio presso il procuratore legale per tutti gli atti inerenti una causa, o presso la sede di lavoro per gli atti relativi ad un concorso pubblico, etc..

Il *domicilio legale* è invece quello dell'incapace di agire. Per il minore, il domicilio è stabilito dalla legge presso la residenza della famiglia; se è sottoposto a tutela, ha il domicilio del tutore, come avviene per l'interdetto. Fino al 1975, anche la donna sposata aveva il domicilio del marito; oggi invece ognuno dei due coniugi ha il proprio domicilio, secondo il criterio ordinario. I coniugi invece stabiliscono d'accordo la comune residenza nella quale si situa il domicilio dei figli minori[(8)].

Dai concetti di domicilio e residenza in senso civilistico, nelle forme fino ad ora citate, si distinguono quelli di residenza fiscale e di *domicilio fiscal*e, come disposto agli artt. 58 e 59 del D.P.R. 29 settembre 1973, n. 600 *("Disposizioni comuni in materia di accertamento delle imposte sui redditi")* e agli artt. 2 e 73 del T.U.I.R. (*"Testo unico delle imposte sui redditi"* - D.P.R. 22 dicembre 1986, n. 917). Per le persone fisiche residenti in Italia, il domicilio fiscale coincide con la residenza anagrafica, le persone fisiche non residenti hanno il domicilio fiscale nel Comune in cui è prodotto il reddito o, se il reddito è prodotto in più Comuni, nel Comune in cui risulta prodotto il reddito più elevato. I soggetti diversi dalle persone fisiche hanno il domicilio fiscale nel Comune in cui si trova la loro sede legale o, in mancanza, la sede amministrativa; se anche questa manca, essi hanno il domicilio fiscale nel Comune ove è stabilita una sede secondaria o una stabile organizzazione e, in mancanza, nel Comune in cui esercitano prevalentemente la loro attività.

(8) Rif: G.IUDICA – P.ZATTI, pagg. 89-90 in *[4]*

Ulteriore tipologia di domicilio, di cui si parlerà nei prossimi capitoli, è il *domicilio* detto *informatico o digitale* inteso quale spazio ideale di pertinenza della persona fisica o giuridica, la cui riservatezza è tutelata in maniera assolutamente analoga rispetto alla riservatezza individuale[(9)].

1.3 La posta elettronica

Si analizzeranno qui le disposizioni normative, che si sono succedute nel tempo, nella volontà del legislatore di procedere ad una generale e fisiologica regolamentazione dell'ammodernamento dell'agire pubblico, sulla base degli strumenti tecnologico-informatici a disposizione della società, in materia di trasmissioni via posta elettronica, partendo dal riconoscimento giuridico della trasmissione digitale.

La **Legge n. 59 del 15 marzo 1997** *("Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa")* sancisce la rilevanza e la validità giuridica del documento informatico e della sua trasmissione con strumenti informatici. In particolare, il comma 2 dell'art. 15, dispone: "*Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*". Questa norma ha introdotto nel nostro ordinamento, da ormai un ventennio, il principio fondamentale della generale rilevanza e della validità dell'attività giuridica svolta in forma elettronica, a prescindere dalla trasposizione dell'atto su supporto cartaceo[(10)].

---

(9) Rif: G.D'AIUTO – L.LEVITA, pagg. 3-5 in *[5]*

(10) Rif: S.CACACE in *[6]*

Nel successivo **D.P.R. 10 novembre 1997, n. 513** *("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della L. 15 marzo 1997, n. 59")* troviamo una prima definizione di indirizzo elettronico all'art. 1, comma 1, lettera l): "*identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici"* e il primo comma dell'art. 12 dello stesso D.P.R. afferma che il documento informatico, trasmesso per via telematica, si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato, fermo restando che quanto trasmesso debba rispettare specifiche regole tecniche volte a garantire integrità, disponibilità e riservatezza delle informazioni ivi contenute, come disposto dall'art. 3 del D.P.R. stesso e dettagliate successivamente nel **D.P.C.M. 8 febbraio 1999** *("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del D.P.R. 10 novembre 1997, n. 513").*

Il **D.P.C.M. 31 ottobre 2000** *("Regole tecniche per la gestione del protocollo informatico da parte delle amministrazioni pubbliche")* prevede, per facilitare la trasmissione dei documenti informatici sia tra le amministrazioni pubbliche che nei rapporti tra amministrazione e cittadini, l'istituzione dell'Indice delle amministrazioni pubbliche e delle aree organizzative omogenee[(11)].

Detto Indice, denominato *IndicePA* o *iPA*, dovrà essere gestito da un sistema informatico accessibile tramite un sito internet[(12)] in grado di permettere la consultazione delle informazioni in esso contenute da parte delle amministrazioni e di tutti i soggetti pubblici o privati. Ciascuna amministrazione, al fine di trasmettere e ricevere documenti informatici soggetti a registrazione di protocollo, deve accreditarsi presso tale Indice ed indicare, per ogni area organizzativa omogenea, la casella di posta elettronica di riferimento.

---

(11) Un'area organizzativa omogenea è un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'art. 2, comma 2, del D.P.R. 428/1998 (come disposto dall'art. 2 del D.P.C.M. 31 ottobre 2000 – "*Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998, n. 428"*).

(12) L'Indice delle amministrazioni pubbliche e delle aree organizzative omogenee è attualmente disponibile all'indirizzo: *http://www.indicepa.gov.it/.*

Il successivo **D.P.R. 28 dicembre 2000, n. 445** *("Testo Unico in materia di documentazione amministrativa"- TUDA),* all'art. 14 (ex art. 12 D.P.R. 10 novembre 1997, n. 513) stabilisce che *"il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato"*[(13)] e che la trasmissione del documento informatico per via telematica equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge; ciò a significare che la notifica telematica è ammessa nei casi in cui la legge ammette la notifica postale[(14)].

La **Legge 16 gennaio 2003, n. 3** *("Disposizioni ordinamentali in materia di pubblica amministrazione")* nell'esplicitare la generale esigenza di semplificazione dell'azione amministrativa, all'art. 27, comma 8, dispone l'emanazione di regolamenti volti all'introduzione nella disciplina vigente, delle norme necessarie all'ampliamento dell'utilizzo di procedure telematiche da parte delle P.A. nella fornitura di servizi ai cittadini e alle imprese, nella contabilità, nell'approvvigionamento di beni e servizi, ed anche per consentire la diffusione e l'uso di strumenti come la posta elettronica tra le pubbliche amministrazioni e nei rapporti tra le pubbliche amministrazioni e i privati.

La **Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003** *("Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni")* ribadisce che uno degli obbiettivi della legislatura è l'adozione della posta elettronica per tutte le comunicazioni e le trasmissioni di documenti interne alla pubblica amministrazione e informa circa l'approvazione di finanziamenti, a favore delle amministrazioni statali, per l'attuazione del progetto @P@[(15)] che prevedeva interventi per la diffusione e l'utilizzo degli strumenti telematici in sostituzione dei canali tradizionali di comunicazione.

---

(13) L'art. 14 del D.P.R. 445/2000 sarà poi abrogato dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005).

(14) Rif: M.IASELLI in *[7]*

(15) Il progetto @p@ promuoveva il cofinanziamento di iniziative per l'introduzione delle comunicazioni elettroniche nelle prassi amministrative della Presidenza del Consiglio dei Ministri, dei Ministeri, delle Forze Armate e delle forze di Polizia, dell'Avvocatura Generale dello Stato, del Consiglio di Stato, della Corte dei Conti e delle Agenzie di cui al D.Lgs. n. 300 del 1999. (Rif: *http://archivio.cnipa.gov.it/site/it-IT/Attivit%C3%A0_-_Archivio_storico/Efficienza_interna_della_PA/*)

La successiva **Direttiva del 4 gennaio 2005** *("Linee guida in materia di digitalizzazione dell'Amministrazione"),* nell'evidenziare che l'utilizzo della posta elettronica è sensibilmente aumentato nelle comunicazioni interne alla P.A., invita le amministrazioni a dare adeguata comunicazione ai fini del completamento dell'*IndicePA,* in corso di predisposizione ad opera del CNIPA[(16)].

La direttiva inoltre informa che molte amministrazioni hanno avviato iniziative per accrescere l'efficienza e ridurre i costi delle proprie attività, sostituendo ad operazioni materiali il ricorso a comunicazioni elettroniche. Infine, se sussistessero ancora incertezze in merito all'utilizzo della posta elettronica, rassicura sulla prossima definitiva approvazione (con il D.P.R. qui a seguire) delle disposizioni necessarie per conferire piena validità giuridica alle comunicazioni per via elettronica, sia all'interno di ciascuna amministrazione, sia tra amministrazioni diverse, sia, infine, tra amministrazioni, cittadini e imprese. Di conseguenza diviene necessario riorganizzare il lavoro all'interno delle amministrazioni per sviluppare l'uso degli strumenti telematici, sostenendo minori oneri per la spedizione e l'archiviazione con notevoli vantaggi di velocità dell'azione amministrativa.

---

(16) **CNIPA**: Centro Nazionale per l'Informatica nella Pubblica Amministrazione.
L'organo, che opera presso la Presidenza del Consiglio dei Ministri, ha più volte cambiato denominazione ma non modificato sostanzialmente le proprie funzioni, per queste ragioni in questo elaborato saranno presenti riferimenti ad AIPA, CNIPA, DigitPA e AgID ma che riferiscono sostanzialmente allo stesso ente. Viene istituito con il Decreto Legislativo n. 39/1993 con il nome di *Autorità per l'informatica nella pubblica amministrazione* (**AIPA**). Si tratta di un organo collegiale costituito dal presidente e da quattro membri, scelti tra persone dotate di alta e riconosciuta competenza e professionalità e di indiscussa moralità e indipendenza. Il presidente è nominato con decreto del presidente del Consiglio dei Ministri, previa deliberazione del Consiglio dei Ministri. Compiti principali dell'Agenzia sono:
- definizione di norme tecniche e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle amministrazioni e delle loro interconnessioni;
- consulenza al Presidente del Consiglio dei Ministri per la valutazione di progetti di legge in materia di sistemi informativi automatizzati.
Successivamente, in attuazione di quanto disposto dal Decreto Legislativo n. 196/2003, l'AIPA è stata trasformata in *Centro nazionale per l'informatica nella pubblica amministrazione* (**CNIPA)**.
In seguito, in attuazione di quanto disposto dal Decreto Legislativo n. 177/2009, il CNIPA ha assunto la denominazione di *Ente nazionale per la digitalizzazione della pubblica amministrazione* **(DigitPA)**, al quale sono trasferite le funzioni del CNIPA.
Attualmente, ai sensi del Decreto Legge n. 83/2012, convertito nella Legge n. 134/2012, DigitPA è stato soppresso ed è stata istituita l'**Agenzia per l'Italia digitale (AgID).** Al sito internet dell'Agenzia ne sono descritte le principali funzioni: *"L'Agenzia per l'Italia Digitale (AgID) coordina le azioni in materia di innovazione per promuovere le tecnologie ICT a supporto della pubblica amministrazione, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea. L'ente eredita le competenze del Dipartimento per la Digitalizzazione e l'Innovazione della Presidenza del Consiglio, dell'Agenzia per la diffusione delle tecnologie per l'innovazione, di DigitPA e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti".* (Rif: *http://www.agid.gov.it*)

1.4 La posta elettronica certificata

Il **D.P.R. 11 febbraio 2005, n. 68** è il regolamento *"Recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3*" che stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione del servizio di Posta Elettronica Certificata (p.e.c.) che consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. Il D.P.R. disciplina l'utilizzo della posta elettronica certificata non solo nei rapporti tra gli uffici della pubblica amministrazione e tra la P.A. e i cittadini ed imprese, ma anche tra privati, ribadendo il valore giuridico della trasmissione di documenti prodotti ed inviati per via telematica.

Gli aspetti contenutistici di questo D.P.R. verranno trattati successivamente, per ora preme evidenziare il disposto dell'art. 3, che modifica il comma 1 dell'art. 14 del D.P.R. 28 dicembre 2000 n. 445 che, in maniera forse un po' semplicistica, a parere di chi scrive, affermava che *"il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato"* e che viene così sostituito: *"Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore"*: la garanzia dell'avvenuta consegna delle e-mail è così posta in capo ai gestori del servizio di posta elettronica certificata che dovranno iscriversi in un apposito elenco tenuto dal CNIPA che, a sua volta, svolgerà funzioni di vigilanza e controllo.

Il **Decreto Legislativo 7 marzo 2005 n. 82,** denominato Codice dell'Amministrazione Digitale (C.A.D.), è stato emanato in attuazione della delega contenuta nell'art. 10 della legge 29 luglio 2003, n. 229 *("Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – Legge di semplificazione 2001").*

Si tratta di un Codice di indubbia rilevanza innovativa e non possiamo che confermare che *"in Italia, contrariamente a quanto di solito accade, il legislatore non ha atteso che i fenomeni si siano consolidati per disciplinarli, ma invece ha cercato di*

anticipare il fenomeno da normare, utilizzando l'emanazione di norme come volano per stimolare la diffusione delle nuove tecnologie"[(17)].

Il Codice affronta in modo organico il tema dell'utilizzo delle tecnologie dell'informazione e della comunicazione: si tratta di un'opera generale di riordino volta all'abbandono delle modalità amministrative più tradizionali e all'accelerazione dei processi di cambiamento ed innovazione in atto. Data la peculiarità della materia trattata, il Codice contribuirà non soltanto a consentire l'erogazione di servizi più efficienti e veloci, ma anche ad avviare forme innovative di partecipazione alla vita amministrativa e politica, tale da avvicinare i destinatari dell'innovazione (cioè i cittadini, le imprese, la società civile) ai suoi *necessariamente* protagonisti (cioè gli amministratori, i funzionari e gli impiegati pubblici), nella nuova amministrazione digitale. L'agire pubblico, con modalità informatiche, dovrebbe dare un contributo rilevante, non solo e non tanto, al pur necessario complessivo ammodernamento delle pubbliche amministrazioni, ma soprattutto comportare, attraverso un più efficace, efficiente e trasparente esercizio delle competenze, un'evoluzione in senso per così dire democratico dei rapporti tra cittadino ed istituzioni[(18)]. Contrariamente a quanto potrebbe sembrare, dal nome attribuito a tale D.Lgs., le norme ivi contenute non sono solo per le pubbliche amministrazioni in quanto, come enunciato nel comma 3 dell'art. 2: "*le disposizioni di cui al capo II concernenti i documenti informatici, le firme elettroniche, i pagamenti informatici, i libri e le scritture, le disposizioni di cui al capo III, relative alla formazione, alla gestione, alla conservazione, nonchè le disposizioni di cui al capo IV relative alla trasmissione dei documenti informatici, si applicano anche ai privati ai sensi dell'articolo 3 del D.P.R. 28 dicembre 2000, n. 445*".

Il C.A.D., entrato in vigore il 1 gennaio 2006, ha subito negli anni diverse modificazioni ed integrazioni[(19)], tra cui certamente le più significative per la tematica trattata in questo scritto, sono avvenute con il Decreto Legislativo n. 235/2010 e il Decreto Legge n. 179/2012 di cui si dirà qui di seguito.

---

(17) Cit: G.FINOCCHIARO in *[8]*

(18) Rif: S.CACACE in *[6]*

(19) Il Codice dell'Amministrazione digitale (Decreto Legislativo 7 marzo 2005 n. 82) ha subìto diverse modificazioni ed integrazioni di cui si riportano gli estremi:
- Decreto legislativo 4 aprile 2006, n. 159 (segue in 19-bis)

Nella sua formulazione originale dispone all'art. 3 primo comma, che "*i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali"*.

L'art. 48 dispone che l'utilizzo della posta elettronica certificata, conformemente alle disposizioni di cui al D.P.R. 11 febbraio 2005, n. 68, consente la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta e la data e l'ora di trasmissione e di ricezione del documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al D.P.R. 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

(19bis) Segue modificazioni ed integrazioni al Codice dell'Amministrazione Digitale:
- Legge 24 dicembre 2007, n. 244
- Decreto-legge 31 dicembre 2007, n. 248 , convertito con modificazioni dalla L. 28 febbraio 2008, n. 31
- Decreto-legge 29 novembre 2008, n. 185 (c.d. "Decreto Anticrisi"), convertito con modificazioni dalla L. 28 gennaio 2009, n.2
- Decreto-legge 30 dicembre 2008, n. 207, convertito con modificazioni, dalla L. 27 febbraio 2009, n. 14
- Legge 18 giugno 2009, n. 69
- Decreto-legge 1 luglio 2009, n. 78, convertito con modificazioni dalla L. 3 agosto 2009, n. 102
- Legge 23 dicembre 2009, n. 191
- Decreto-legge 30 dicembre 2009, n. 194, convertito con modificazioni dalla L. 26 febbraio 2010, n. 25
- Decreto legislativo 27 gennaio 2010, n. 32
- Decreto legislativo 2 luglio 2010, n. 104
- Decreto-legge 29 dicembre 2010, n. 225, convertito con modificazioni dalla L. 26 febbraio 2011, n. 10
- Decreto legislativo 30 dicembre 2010, n. 235 – "Nuovo codice dell'Amministrazione digitale"
- Decreto-legge 13 agosto 2011, n. 138, convertito con modificazioni dalla L. 14 settembre 2011, n. 148
- Decreto-legge 6 dicembre 2011, n. 201 (c.d. "salva Italia"), convertito con modificazioni dalla L. 22 dicembre 2011, n. 214
- Decreto-legge 9 febbraio 2012, n. 5, convertito con modificazioni dalla L. 4 aprile 2012, n. 35
- Decreto-legge 22 giugno 2012, n. 83, convertito con modificazioni dalla L. 7 agosto 2012, n. 134
- Decreto-legge 6 luglio 2012, n. 95, convertito con modificazioni dalla L. 7 agosto 2012, n. 135
- Decreto-legge 18 ottobre 2012, n. 179 (c.d. "Decreto Crescita 2.0"), convertito con modificazioni dalla L. 17 dicembre 2012, n. 221
- Decreto legislativo 14 marzo 2013, n. 33
- Decreto-legge 21 giugno 2013, n. 69 (c.d. "Decreto del Fare"), convertito con modificazioni dalla L. 9 agosto 2013, n. 98
- Legge 27 dicembre 2013, n. 147.

Le trasmissioni di documenti tra le pubbliche amministrazioni devono avvenire, come disposto dal primo comma dell'art. 47 del Codice, *di norma* mediante l'utilizzo della posta elettronica e sono valide, ai fini del procedimento amministrativo, quando ne sia verificata la provenienza. Il secondo comma del medesimo articolo dispone, tra gli strumenti atti a verificare la provenienza, l'utilizzo di sistemi di posta elettronica certificata di cui al D.P.R. 11 febbraio 2005, n. 68. Le P.A. inoltre, entro ventiquattro mesi dalla data di entrata in vigore del Codice, devono istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata per ciascun registro di protocollo ed utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Il **Decreto del Ministro per l'Innovazione e le Tecnologie del 2 novembre 2005** contiene le *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"* e dettaglia i requisiti tecnico-funzionali che devono essere rispettati dalle piattaforme utilizzate dai gestori per erogare il servizio.

La **Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005,** rivolta alle pubbliche amministrazioni, ricorda che sussistono gli strumenti tecnico-giuridici attraverso cui ripensare la propria organizzazione in chiave digitale al fine di fornire a cittadini ed imprese i propri servizi *on line* realizzando, nel contempo, una progressiva riduzione dei costi ed un incremento dell'efficienza e della trasparenza. Tra questi strumenti viene citata la posta elettronica ed in particolare vengono invitate le pubbliche amministrazioni a "rendersi facilmente raggiungibili telematicamente" attraverso l'esposizione nei propri siti internet istituzionali degli indirizzi di posta elettronica e posta elettronica certificata in quanto, come già disposto dal C.A.D., i cittadini e le imprese hanno il diritto di chiedere e ottenere l'uso delle tecnologie informatiche.

La **circolare CNIPA n. 49 del 24 novembre 2005** definisce le modalità con cui i soggetti, pubblici e privati che intendono esercitare l'attività di gestori di posta

elettronica certificata, devono presentare le domande di iscrizione all'elenco pubblico dei gestori e i requisiti tecnico-organizzativi che essi devono possedere (ai sensi dell'art. 14 del D.P.R. 11 febbraio 2005, n. 68); a seguire la **circolare CNIPA n. 51 del 7 dicembre 2006** indica le modalità attraverso le quali il CNIPA svolge le funzioni di vigilanza e di controllo sulle attività esercitate dagli iscritti nell'elenco. In particolare il CNIPA deve curare il monitoraggio di eventuali casi di esercizio o pubblicizzazione dell'attività di gestore da parte di soggetti non abilitati, verificare l'interoperabilità dei sistemi di PEC utilizzati dai gestori, controllare il possesso e il mantenimento dei requisiti previsti per l'iscrizione nell'elenco, vigilare sulle modalità di vendita dei servizi di PEC attraverso canali commerciali e controllare i livelli di servizio erogati anche attraverso sopralluoghi presso le strutture utilizzate dai gestori.

La **Legge n. 244 del 24 dicembre 2007** *("Legge Finanziaria 2008"),* in un'ottica di riduzione delle spese di invio della corrispondenza cartacea da parte delle P.A., all'art. 2 comma 589, dispone che il CNIPA effettui, anche a campione, azioni di monitoraggio e verifica del rispetto delle disposizioni di cui all'art. 47 del C.A.D. *("le trasmissioni di documenti tra le pubbliche amministrazioni devono avvenire di norma attraverso la posta elettronica certificata").* Il mancato adeguamento alle predette disposizioni in misura superiore al 50 per cento del totale della corrispondenza inviata, certificato dal CNIPA, comporta per le pubbliche amministrazioni dello Stato, comprese le aziende e le amministrazioni dello Stato ad ordinamento autonomo e gli enti pubblici non economici nazionali, la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di invio della corrispondenza cartacea.

Il **Decreto Legge n. 185 del 29 novembre 2008** *("Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale"*, convertito in legge con modificazioni dall'art. 1 della Legge 28 gennaio 2009 n. 2) all'art. 16 rende obbligatoria la dotazione di una casella di posta elettronica certificata per le imprese costituite in forma societaria e per i professionisti iscritti ad albi. Le imprese costituite in forma societaria sono tenute ad indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al Registro delle imprese mentre le società già costituite, hanno tre anni di tempo

dall'entrata in vigore della legge per indicare la propria casella di posta elettronica certificata al Registro. I professionisti iscritti in albi ed elenchi, istituiti con legge dello Stato, comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata entro un anno dalla data di entrata in vigore del decreto. Gli ordini ed i collegi a loro volta, pubblicano in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata. La consultazione per via telematica dei singoli indirizzi di posta elettronica certificata nel Registro delle imprese o negli albi o elenchi costituiti, avviene liberamente e senza oneri; l'estrazione di elenchi di indirizzi è consentita, alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza. Nella Circolare n. 3645/C del 3 novembre 2011 del Ministero dello Sviluppo Economico, contenente le indicazioni operative relative alla comunicazione della p.e.c., è indicato comunque "*che nulla osti all'indicazione, nell'ambito della comunicazione in questione, dell'indirizzo di posta elettronica di uno studio professionale che assista l'impresa negli adempimenti burocratici, ovvero, ad esempio, di un'altra società cui l'impresa obbligata all'adempimento sia giuridicamente o economicamente collegata*".

Particolarmente significativo è che le comunicazioni tra i soggetti detti, cioè tra le amministrazioni pubbliche, le imprese costituite in forma societaria e i professionisti, che abbiano provveduto agli adempimenti previsti, potranno essere inviate attraverso posta elettronica certificata, senza che il destinatario debba dichiarare la disponibilità ad accettarne l'utilizzo. Poiché i suddetti adempimenti consistono sostanzialmente nella regolare pubblicazione dell'indirizzo p.e.c., tra queste categorie di soggetti non è necessario ottenere dal destinatario una preventiva dichiarazione di disponibilità, perché questa è implicita nella pubblicazione dell'indirizzo di posta elettronica certificata.

Il comma 5 dell'art. 16-bis del D.L. dispone inoltre che, data la priorità di massima diffusione delle tecnologie telematiche nelle comunicazioni già prevista nel Codice dell'Amministrazione Digitale, ai cittadini che ne fanno richiesta, è attribuita una casella di posta elettronica certificata il cui utilizzo avviene ai sensi degli artt. 6 e 48 del C.A.D., con effetto equivalente, ove necessario, alla notificazione per mezzo della posta; le comunicazioni che transitano per la predetta casella di posta elettronica certificata sono senza oneri.

Ogni amministrazione pubblica utilizza, per le comunicazioni e le notificazioni aventi come destinatari i dipendenti della stessa o di altra amministrazione pubblica, unicamente la posta elettronica certificata, ai sensi dei citati artt. 6 e 48 con effetto equivalente, ove necessario, alla notificazione per mezzo della posta.

Il **D.P.C.M. 6 maggio 2009** definisce le modalità con cui il cittadino può richiedere l'attivazione e il rilascio di un indirizzo di posta elettronica certificata, valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni, ai sensi dell'art 16-bis del D.L. 29 novembre 2008, n. 185. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, direttamente o tramite l'affidatario del servizio, assegna un indirizzo p.e.c. al richiedente. L'affidatario rende consultabili, in via telematica alle pubbliche amministrazioni, tali indirizzi nel rispetto dei criteri di qualità, sicurezza ed interoperabilità definiti dal CNIPA e nel rispetto della disciplina in materia di tutela dei dati personali di cui al Decreto Lgs. 30 giugno 2003, n. 196. Al contempo il D.P.C.M. ribadisce la necessità che le P.A. istituiscano una casella di posta elettronica certificata per ogni registro di protocollo, ne diano comunicazione al CNIPA e forniscano sui loro siti istituzionali adeguata informazione per consentire l'inoltro di istanze da parte dei cittadini titolari di p.e.c..

La **Circolare CNIPA n. 56 del 21 maggio 2009,** che abroga e sostituisce la circolare n. 49 del 24 novembre 2005, è emanata ai sensi del già citato D.M. 2 novembre 2005 e definisce in maniera puntuale le modalità con le quali i soggetti pubblici e privati, che intendono esercitare l'attività di gestori di posta elettronica certificata, devono presentare domanda al CNIPA.

Con l'art. 33 della **Legge 18 giugno 2009 n. 69** *("Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile")* vengono disposti 15 criteri di delegazione al Governo per l'adozione di decreti legislativi volti a modificare il C.A.D., tra cui la previsione di forme sanzionatorie per le P.A. che non ottemperano alle prescrizioni del Codice stesso. L'art. 34 di detta legge dispone due significative modifiche al C.A.D. in materia di posta elettronica certificata.

La prima modifica è all'art. 6 (rubricato: "*utilizzo della posta elettronica certificata"*) dove viene aggiunto il comma 2-bis che dispone che le pubbliche

amministrazioni regionali e locali possano assegnare ai cittadini residenti, delle caselle di posta elettronica certificata atte alla trasmissione di documentazione ufficiale. Tale integrazione è stata successivamente abrogata dal D.Lgs. 30 dicembre 2010, n. 235.

La seconda modifica è all'art. 54 del C.A.D. in materia di contenuto dei siti delle pubbliche amministrazioni: *"entro il 30 giugno 2009, le amministrazioni pubbliche che già dispongono di propri siti sono tenute a pubblicare nella pagina iniziale del loro sito un indirizzo di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta"*, anche questa integrazione è stata successivamente rimossa con il D.Lgs 14 marzo 2013, n. 33 e l'art. 54 del C.A.D. si è così trasformato*: "I siti delle pubbliche amministrazioni contengono i dati di cui al decreto legislativo recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, adottato ai sensi dell'articolo 1, comma 35, della legge 6 novembre 2012, n. 190"*.

Nell'art. 35 della stessa Legge n. 69/2009 il legislatore si pone il problema dell'interoperabilità della p.e.c. italiana con analoghi sistemi internazionali e modifica il disposto degli articoli del D.L. n. 185/2008, che obbligano alla titolarità di un indirizzo di posta elettronica certificata le aziende e i professionisti iscritti ad albi, indicando che in alternativa all'indirizzo p.e.c., essi possono comunicare un *"analogo 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"*.

La Legge 3 agosto 2009, n. 102 *("Conversione in legge, con modificazioni, del decreto-legge 1° luglio 2009, n. 78, recante provvedimenti anticrisi, nonché proroga di termini e della partecipazione italiana a missioni internazionali")* interviene nel Codice dell'Amministrazione Digitale introducendo l'art. 57-bis e modificando l'art. 65.

Allo scopo di assicurare la trasparenza delle attività istituzionali, con l'introduzione dell'art. 57-bis, si definiscono in dettaglio i contenuti dell'Indice delle amministrazioni pubbliche (IndicePA), nel quale sono indicati la struttura organizzativa, l'elenco dei servizi offerti e le informazioni relative al loro utilizzo, gli indirizzi di posta elettronica da utilizzare per le comunicazioni, per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge fra le amministrazioni e fra le amministrazioni ed i cittadini; al CNIPA è affidata la realizzazione e la gestione di detto

Indice per il quale si applicano le regole tecniche di cui al D.P.C.M. 31 ottobre 2000. Le amministrazioni aggiornano gli indirizzi ed i contenuti dell'Indice con cadenza almeno semestrale, salvo diversa indicazione del CNIPA. La mancata comunicazione degli elementi necessari al completamento dell'Indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

Le istanze e le dichiarazioni, presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici, sono valide secondo quanto disposto dalla neo-introdotta lettera c-bis all'art. 65, comma 1, anche quando "*l'autore è identificato dal sistema informatico attraverso le credenziali di accesso relative all'utenza personale di posta elettronica certificata di cui all'articolo 16-bis del D.L. 29 novembre 2008, n. 185, convertito con modificazioni, dalla legge 28 gennaio 2009, n. 2"*.

Il **Decreto Legislativo 30 dicembre 2010, n. 235** *("Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'art. 33 della legge 18 giugno 2009, n. 69")* ha ampiamente modificato il C.A.D., tant'è che dall'entrata in vigore delle modifiche, il Codice è stato denominato "Nuovo Codice dell'Amministrazione Digitale". Particolarmente rilevanti sono le modifiche in materia di posta elettronica certificata: la p.e.c. diventa per tutte le imprese e i professionisti, che per legge devono esserne dotati, e per i cittadini che lo desiderano, il mezzo più veloce, sicuro e valido per comunicare con le amministrazioni pubbliche. Viene ribadito l'obbligo per le pubbliche amministrazioni di utilizzo della p.e.c. per tutte le comunicazioni in cui sia necessaria una ricevuta di invio e una di consegna con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata[(20)].

Andando a dettagliare le modifiche, per la materia qui di interesse, innanzitutto l'art. 1 del C.A.D. viene integrato con due definizioni: quella di posta elettronica certificata, definita come un "*sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi*" e quella di gestore di posta elettronica certificata cioè "*il soggetto*

(20) Rif: L.FOGLIA - F.GIANNUZZI in *[10]*

che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata".

All'art. 2 è stato esteso l'ambito soggettivo di applicazione del C.A.D. in quanto le specifiche disposizioni del Codice che fino a quel momento si applicavano solo alle pubbliche amministrazioni, ora vengono estese anche alle società "*interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione come individuate dall'ISTAT ai sensi dell'art. 1, comma 5 della legge 30 dicembre 2004, n. 31"*.

In merito alle comunicazioni tra imprese e amministrazioni pubbliche, il digitale diventa la regola in quanto il neo-introdotto art. 5-bis dispone: "*La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese"*, fermo restando che quanto disposto dovrà essere poi declinato con riferimento alle specifiche comunicazioni e agli obblighi posti dalle specifiche disposizioni del Codice per la comunicazione: ad esempio firma digitale, posta elettronica certificata, ecc.[(21)].

DigitPA provvederà alla verifica dell'attuazione della disposizione secondo le modalità e i termini indicati in quello che sarà il decreto di attuazione. Sono introdotte inoltre nuove disposizioni in materia di controllo dei gestori dei servizi di posta certificata, in particolare viene modificato l'art. 31 del Codice che dispone la vigilanza e il controllo a cura di DigitPA non più solo sull'attività dei certificatori, cioè sui soggetti che prestano servizi di certificazione di firme elettroniche, ma anche sui gestori di posta elettronica certificata. E' stato altresì introdotto l'art. 32-bis che prevede sanzioni per i certificatori qualificati e per i gestori di p.e.c. che non siano in grado di offrire garanzie sul servizio reso o non diano adeguata comunicazione a DigitPa e agli utenti, in merito al verificarsi di eventuali malfunzionamenti.

---

(21) Cit: G.FINOCCHIARO in *[9]*

Dall'art. 45 del C.A.D. viene rimosso il fax tra i mezzi di trasmissione di documenti ad una pubblica amministrazione idonei ad accertarne la fonte di provenienza.

In merito poi, alla trasmissione dei documenti tra le pubbliche amministrazioni, il primo comma dell'art. 47, fino alle modificazioni introdotte da questo D.Lgs., disponeva: "*Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza*", con questo D.Lgs., vengono rimosse le parole "*di norma*" proprio a rafforzare la trasmissione informatizzata dei documenti; viene inoltre aggiunta la *cooperazione applicativa*[(22)] come ulteriore strumento di comunicazione tra le pubbliche amministrazioni.

L'art. 48 comma 2 disponeva, prima delle modifiche qui intervenute, che la trasmissione di documenti informatici effettuata mediante la posta elettronica certificata equivale "*nei casi consentiti dalla legge*" alla notificazione per mezzo della posta, nella nuova formulazione invece la trasmissione via p.e.c. equivale "*salvo che la legge disponga diversamente*", alla notificazione per mezzo della posta.

[(22)] L'art. 72 del C.A.D. definisce la cooperazione applicativa: "*la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi*".

Cooperazione applicativa già ampiamente attiva in ambito regionale: si legge, dal Rapporto ICAR del 2008, che l'interoperabilità e la cooperazione applicativa afferiscono ad una specifica capacità di due o più sistemi informativi connessi in rete di disporre automaticamente, per le proprie finalità applicative, dei dati che sono producibili e/o acquisibili attraverso il processo elaborativo delle applicazioni operanti in altri sistemi informativi.

In altre parole, un'applicazione in grado di cooperare può – nel corso del suo processo elaborativo – far uso di un'informazione elaborata da un'altra applicazione (è questo il caso, ad esempio, di un applicativo sanitario che può richiedere i dati anagrafici di un cittadino, al sistema di anagrafe civile del comune di residenza del cittadino). Quando ciò avviene in modo automatico si realizza la cooperazione applicativa in rete. Ciò comporta l'attivazione di infrastrutture principalmente di tipo logico (software) per l'interoperabilità, nonché l'estensione delle funzioni dell'applicazione esistente per il trattamento dei dati oggetto di scambio con le applicazioni operanti negli altri sistemi informativi, secondo le specifiche finalità della cooperazione applicativa. Garantire l'interoperabilità e la cooperazione applicativa tra i sistemi informativi della P.A. centrale e locale è diventato quindi un requisito di primaria importanza, al fine di realizzare il pieno ed efficace sviluppo dell'e-government. Ciò risponde a due esigenze principali: integrare i processi automatizzati di back-office per l'erogazione di servizi interni (da una PA all'altra) ed esterni (dalla P.A. verso i cittadini) ed erogare servizi finali integrati in rete al cittadino in modo trasparente ed unitario. (Rif: *Interoperabilità e Cooperazione Applicativa nelle Regioni italiane – Due anni di lavoro*. Pubblicazione di ottobre 2008, pagg. 33-40, su *http://www.progettoicar.it*)

Le amministrazioni devono istituire e pubblicare nell'IndicePA almeno una casella di posta elettronica certificata per ciascun registro di protocollo, come disposto dalle modificazioni all'art. 47 comma 3 e, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano. La consultazione degli indirizzi di posta elettronica certificata (di cui agli artt. 16 comma 10 e 16-bis comma 5 del D.L. 185/2008, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2) e l'estrazione di elenchi dei suddetti indirizzi da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali.

Infine viene ulteriormente modificato il comma 1 dell'art. 57-bis che riduce l'elenco delle informazioni che le amministrazioni devono pubblicare in IndicePA: *"Al fine di assicurare la trasparenza delle attività istituzionali è istituito l'indice degli indirizzi delle amministrazioni pubbliche, nel quale sono indicati gli indirizzi di posta elettronica da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge fra le amministrazioni e fra le amministrazioni ed i cittadini"*.

Il **Decreto del Presidente del Consiglio dei Ministri del 22 luglio 2011** *("Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni")* dispone all'art. 1, in merito alle comunicazioni tra imprese e amministrazioni pubbliche, che a decorrere dal 1° luglio 2013, la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici avvengono esclusivamente in via telematica. All'art. 3 viene altresì specificatamente sancito che a decorrere dal 1° luglio 2013, le pubbliche amministrazioni non possono accettare o effettuare in forma cartacea le comunicazioni ad altre amministrazioni o ad imprese; inoltre, a decorrere dalla stessa data, in tutti i casi in cui non è prevista una diversa modalità di comunicazione telematica, le comunicazioni avvengono mediante l'utilizzo della posta elettronica certificata.

Il decreto definisce gli step procedurali che le amministrazioni centrali devono rispettare e che consistono nella definizione di un programma di informatizzazione delle comunicazioni con le imprese fissando obiettivi intermedi quantitativamente omogenei a cadenza almeno semestrale e, ad ogni scadenza, la pubblicazione sui siti istituzionali di ciascuna amministrazione dell'elenco dei procedimenti amministrativi per i quali le comunicazioni di cui all'art. 1 sono svolte esclusivamente in via telematica, con l'indicazione della data di decorrenza, comunque non superiore a sessanta giorni.

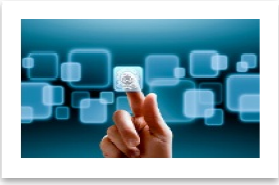
Il **Decreto legge 9 febbraio 2012, n. 5** *("Disposizioni urgenti in materia di semplificazione e di sviluppo"*, convertito con modificazioni dalla Legge 4 aprile 2012, n. 35) effettua anch'esso diverse modificazioni al C.A.D. ed in particolare, per la materia qui trattata, si segnala rettificato il comma 3 dell'art. 57-bis, in quanto si dispone che le amministrazioni aggiornino gli indirizzi p.e.c. e contenuti dell'Indice degli indirizzi delle pubbliche amministrazioni non più con cadenza semestrale ma in maniera tempestiva.

Allo scopo di incentivare e favorire il processo di informatizzazione e di potenziamento ed estensione dei servizi telematici, si aggiunge inoltre il comma 3-bis all'art. 63 che impone l'obbligo, ai soggetti già individuati ai sensi dell'art. 2 comma 2 dello stesso Codice, a partire dal 1 gennaio 2014, di avvalersi esclusivamente di canali e servizi telematici, ivi inclusa la posta elettronica certificata, per l'utilizzo dei propri servizi, anche a mezzo di intermediari abilitati, per la presentazione da parte degli interessati di denunce, istanze, atti e garanzie fideiussorie, per l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi, nonché per la richiesta di attestazioni e certificazioni.

Si segnala infine l'introduzione del comma 6-bis all'art. 16 del D.L. n. 185/2008, con il quale viene previsto che le imprese, costituite in forma societaria, che ometteranno l'indicazione del proprio indirizzo di posta elettronica certificata vedranno sospendersi per tre mesi la domanda di iscrizione all'Ufficio del Registro delle Imprese, in attesa dell'integrazione.

1.5 Il domicilio digitale

Tra le molte novità introdotte dal **Decreto Legge 18 ottobre 2012, n. 179** *("Ulteriori misure urgenti per la crescita del Paese"* - convertito con modificazioni dalla legge 17 dicembre 2012, n. 221), trova collocazione il domicilio digitale.



L'art. 4 di questo decreto dispone l'introduzione dell'art. 3-bis nel C.A.D, rubricato *"domicilio digitale del cittadino"* con lo scopo di facilitare la comunicazione tra le pubbliche amministrazioni e i cittadini.

La relazione illustrativa di accompagnamento al decreto legge afferma che *"la disponibilità del domicilio digitale, costituito da una casella di posta elettronica (certificata) o da una casella certificata governativa indicata dal cittadino stesso e custodita nell'ANPR*[(23)]*, consente alle amministrazioni pubbliche di digitalizzare le comunicazioni verso il cittadino e di indirizzarle al domicilio digitale conosciuto dall'intero sistema, con notevoli risparmi dovuti all'eliminazione della carta e delle spese di invio"*.

Con la Legge di conversione n. 221/2012, tuttavia, si è ritenuto che solamente le caselle di posta elettronica certificata cosiddette *governative*, cioè rilasciate ai sensi ai sensi dell'art. 16-bis, comma 5, del D.L. 185/2008, convertito con modificazioni dalla Legge n. 2/2009, possano costituire domicilio digitale. Detto indirizzo di posta elettronica certificata, indicato dal cittadino, sarà inserito nell'Anagrafe Nazionale della Popolazione Residente e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi. Con decreto del Ministro dell'Interno, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro delegato per l'innovazione tecnologica, sentita l'Agenzia per l'Italia digitale, dovranno essere definite le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino, nonché le modalità di consultazione dell'ANPR da parte dei gestori o esercenti di pubblici servizi ai fini del reperimento del domicilio digitale dei propri utenti.

---

(23) ANPR - Anagrafe nazionale della popolazione residente ai sensi dell'art. 62 del C.A.D. vigente: è una base di dati di interesse nazionale, istituita presso il Ministero dell'interno che subentra con un piano graduale, da completare entro il 31 dicembre 2014, all'Indice Nazionale delle Anagrafi (INA) e all'Anagrafe della Popolazione Italiana Residente all'Estero (AIRE).

A meno che non sia prevista dalla normativa vigente una diversa modalità di comunicazione o di pubblicazione in via telematica, a decorrere dal 1° gennaio 2013, le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato, anche ai sensi dell'art. 21-bis della Legge 7 agosto 1990, n. 241 (in materia di provvedimenti limitativi della sfera giuridica dei privati), senza oneri di spedizione a suo carico.

"Ogni altra forma di comunicazione non potrà produrre effetti pregiudizievoli per il destinatario", ciò a significare che, per coloro che dispongono di un domicilio digitale, questo deve essere l'unico canale che la P.A. e i gestori o esercenti di pubblici servizi utilizzano per comunicare e al contempo, per i cittadini stessi comporta l'obbligo di consultare la propria casella p.e.c..

L'obbligo, per le aziende e per i professionisti iscritti ad albi, di dotarsi di una casella di posta elettronica certificata, già disposto dal D.L. n. 185/2008, è esteso alle imprese individuali che si iscrivono al Registro delle imprese o all'Albo delle imprese artigiane, che sono tenute a depositare, presso l'Ufficio del Registro delle imprese competente, il proprio indirizzo di posta elettronica certificata entro il 30 giugno 2013.

L'Ufficio del Registro delle imprese, che riceve una domanda di iscrizione da parte di un'impresa individuale, che non deposita il proprio indirizzo di posta elettronica certificata, sospende la domanda per tre mesi, in attesa che essa sia integrata con l'indirizzo di posta elettronica certificata.

Con lo stesso D.L. n. 179/2012 viene introdotto nel C.A.D. l'art. 6-bis, che istituisce il pubblico elenco denominato Indice Nazionale degli Indirizzi di Posta Elettronica Certificata (INI-PEC) delle imprese e dei professionisti, istituito presso il Ministero per lo Sviluppo Economico.

Tale indice è realizzato a partire dagli elenchi p.e.c. costituiti presso il Registro delle imprese e gli ordini o collegi professionali (secondo quanto già disposto dall'art. 16 del D.L. 185/2008, convertito con modificazioni dalla legge n. 2/2009). L'accesso all'INI-PEC è consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web e senza necessità di autenticazione.

Detto Indice è costituito da una base informativa in formato aperto[(24)].

Il **Decreto 19 marzo 2013** del Ministero per lo sviluppo economico stabilisce la modalità di realizzazione e gestione operativa dell'INI-PEC, nonché le modalità di accesso allo stesso, le modalità e le forme con cui gli ordini ed i collegi professionali comunicano e aggiornano gli indirizzi di posta elettronica certificata relativi ai professionisti di propria competenza. Con tale decreto, l'art. 57-bis del C.A.D., che tratta del già istituito Indice degli indirizzi delle pubbliche amministrazioni, viene nuovamente modificato, in quanto devono esservi pubblicati anche i gestori dei pubblici servizi con i relativi indirizzi di posta elettronica certificata da utilizzare per le comunicazioni, per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge, tra le pubbliche amministrazioni, i gestori di pubblici servizi ed i privati. Nel decreto viene nuovamente ribadito che la trasmissione di documenti tra le pubbliche amministrazioni, deve avvenire attraverso la posta elettronica, come già disposto dall'art. 47 del C.A.D., articolo a cui viene aggiunto il comma 1-bis che, ferma restando l'eventuale responsabilità per danno erariale, dispone la responsabilità dirigenziale e disciplinare in caso di inosservanza.

Il **Decreto Legge 21 giugno 2013, n. 69** (*"Disposizioni urgenti per il rilancio dell'economia"* convertito con modificazioni dalla Legge 9 agosto 2013, n. 98*)*, interviene nuovamente in materia di domicilio digitale. L'art. 14, con riferimento alle misure per favorirne la diffusione, modifica l'art. 10 del D.L. 13 maggio 2011, n. 70 *("Semestre Europeo – Prime disposizioni urgenti per l'economia convertito con modificazioni dalla L. 12 luglio 2011, n. 106")* disponendo che, all'atto della richiesta del documento unificato, ovvero all'atto dell'iscrizione anagrafica o della dichiarazione di cambio di residenza a partire dall'entrata a regime dell'Anagrafe Nazionale della Popolazione Residente, è assegnata al cittadino una casella di posta elettronica certificata (di cui all'art. 16-bis comma 5 del D.L. n. 185/2008) con la funzione di domicilio digitale ai sensi dell'art. 3-bis del C.A.D..

[(24)] Il formato dei dati digitali si definisce "aperto" quando ne viene resa pubblica, mediante esaustiva documentazione, la sintassi, la semantica, il contesto operativo e le modalità di utilizzo. Tali informazioni, unitamente ad una guida all'uso del formato, orientata alla lettura da parte dell'utilizzatore, devono essere presenti in uno o più documenti rilasciati dall'ente proponente lo standard.

Tale casella sarà successivamente attivabile in modalità telematica dal medesimo cittadino.

Nello stesso Decreto legge 69/2013 si dispone che, con successivo decreto del Ministro dell'Interno, siano stabilite le modalità di rilascio del domicilio digitale all'atto di richiesta del documento unificato[25]. Inoltre, in materia di trasmissioni di documenti si aggiunge, all'47 del C.A.D., la specifica che *"è in ogni caso esclusa la trasmissione di documenti a mezzo fax"* tra le pubbliche amministrazioni.

Il **D.P.C.M. 23 agosto 2013, n. 109** è il regolamento contenente le disposizioni per la prima attuazione dell'Anagrafe Nazionale della Popolazione Residente. Il decreto definisce le fasi progettuali con cui sarà istituita questa base di dati di interesse nazionale[26] che subentra all'INA, all'AIRE e, gradualmente, alle Anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni, sulla base di un apposito piano da completarsi entro il 31 dicembre 2014. Tale decreto, dispone, in materia di domicilio digitale, all'art. 2 comma 2, che l'ANPR renda disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi l'indirizzo p.e.c. indicato dal cittadino quale proprio domicilio digitale.

---

[25] La legislazione attuale prevede la realizzazione del documento digitale unificato (DDU). Tale documento elettronico, che sostituisce la carta di identità e la tessera sanitaria, consente di dotare tutti i cittadini di un valido strumento per l'accesso ai servizi in rete. Il progetto prevede l'utilizzo di smart card con un doppio microprocessore, a radiofrequenza e a contatti. La presenza del chip a contatti, destinato in futuro ad essere eliminato, consente di garantire la continuità dei servizi attualmente forniti attraverso la Carta Nazionale dei Servizi (e carte a questa conformi) per un adeguato periodo di tempo affinché siano resi disponibili i servizi attraverso il chip contactless. Nel corso del progetto, che prevede l'emanazione di due decreti, si è stabilito che le regole tecnologiche siano pubblicate in rete a cura del Ministero dell'Interno. (Rif: *http://www.agid.gov.it/identita-digitali/documento-digitale-unificato*)

[26] Una base di dati di interesse nazionale è costituita, secondo l'art. 60 del C.A.D., dall'insieme delle informazioni raccolte e gestite digitalmente dalle P.A., omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni, anche per fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti. Esse costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni.
Attualmente (con gli aggiornamenti intervenuti con la L. 147/2013) le basi di dati di interesse nazionale sono:
a) repertorio nazionale dei dati territoriali;
b) anagrafe nazionale della popolazione residente;
c) banca dati nazionale dei contratti pubblici di cui all'art. 62-bis;
d) casellario giudiziale;
e) registro delle imprese;
f) archivi automatizzati in materia di immigrazione e di asilo di cui all'art. 2, comma 2, del D.P.R. 27 luglio 2004, n. 242.

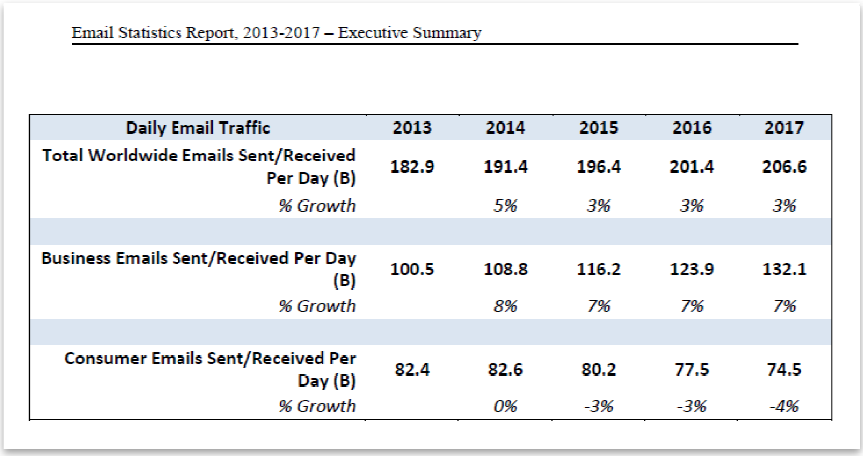
A conclusione dell’excursus normativo svolto in questo capitolo, in materia di domicilio, posta elettronica e posta elettronica certificata, pare tuttavia doveroso evidenziare che, al momento in cui si scrive, non esistono regolamenti attuativi in merito alle modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale e non risultano definite le modalità con cui la pubblica amministrazione, i gestori o gli esercenti pubblici servizi possano consultare l'ANPR (attualmente in corso di costituzione) per reperire il domicilio digitale dei cittadini.

2. La certificazione della spedizione

Il numero di comunicazioni via posta elettronica raggiungono ormai quotidianamente cifre esorbitanti[(26)]. In Italia le e-mail inviate ogni anno sono più di una decina di miliardi[(27)], anche se esiste un notevole divario rispetto agli altri paesi europei in termini soprattutto di minore diffusione dell'e-commerce e dell'e-government. Nel 2012 solo il 15% dei cittadini italiani effettuava acquisti on-line, rispetto a una media europea del 43%, mentre la percentuale di coloro che interagivano on-line con la pubblica amministrazione era dell'8% nel nostro Paese e del 21% nell'Unione Europea[(28)].

---

(26) La tabella sottostante rappresenta, in miliardi, il numero delle e-mail inviate giornalmente a livello mondiale con le previsioni di incremento annuali:



Email Statistics Report, 2013-2017 – Executive Summary

Daily Email Traffic	2013	2014	2015	2016	2017
Total Worldwide Emails Sent/Received Per Day (B)	182.9	191.4	196.4	201.4	206.6
% Growth		*5%*	*3%*	*3%*	*3%*
Business Emails Sent/Received Per Day (B)	100.5	108.8	116.2	123.9	132.1
% Growth		*8%*	*7%*	*7%*	*7%*
Consumer Emails Sent/Received Per Day (B)	82.4	82.6	80.2	77.5	74.5
% Growth		*0%*	*-3%*	*-3%*	*-4%*

(Immagine da: THE RADICATI GROUP, INC., Email Statistics Report, 2013 -2017, *http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf*)

Si prevede, inoltre, che il numero totale di account di posta elettronica in tutto il mondo arrivi ad oltre 4,9 miliardi entro la fine del 2017. (Rif: The Radicati Group, Inc.: *http://www.radicati.com*)

(27) In Italia, una delle aziende leader nel settore dell'e-mail marketing, ha pubblicato un'analisi basata sui dati aggregati provenienti da tutti gli invii dei propri clienti relativamente all'anno 2013: sono quasi 12 miliardi le e-mail inviate in un anno di cui il 69% newsletter, il 30,08% DEM (Direct Email Marketing) e lo 0,2% transazionali (mail con contenuto personalizzato inviate a singoli destinatari che comunicano l'attivazione di un servizio, la conferma di una registrazione, l'invio di una fattura, ecc..).
(Rif: MailUp, *http://www.mailup.it/risorse/email-marketing-statistics-2013.pdf*).

(28) La relazione di accompagnamento del Decreto Legge 18 ottobre 2012, n. 179 (c.d. *"Decreto Crescita 2.0"*), nel riportare tali percentuali, si pone come obbiettivo quello di permettere all'Italia di colmare il divario esistente con gli altri paesi europei in materia di e-commerce ed e-government.
(Rif: G.FINOCCHIARO in *[11]*)

Seppure in materia di e-commerce ed e-government l'Italia è al di sotto della media europea, non è certo negabile la normalità, semplicità e immediatezza con cui inviamo e riceviamo e-mail nella nostra quotidianità. Dire oggi che le e-mail sono documenti informatici, potrebbe sembrare cosa ovvia, tuttavia si ritiene necessario in questo capitolo, trattare innanzitutto il tema della valenza giuridica del documento informatico e delle firme elettroniche che ad esso possono essere connesse, proprio per andare a "collocare" giuridicamente le comunicazioni via posta elettronica.

Ciò che si intende evidenziare è che l'e-mail, proprio per le sue peculiarità tecniche, non fornisce certezze giuridiche in merito all'identità del mittente, all'integrità dei contenuti e non dà garanzia dell'avvenuta trasmissione e ricezione avvallate da una collocazione temporale certa. Il legislatore italiano, allo scopo di fornire piene certezze alle comunicazioni elettroniche, ha scelto di istituire la posta elettronica certificata, dettagliandone vincoli giuridici e informatici, tali da fornire quelle garanzie che la posta elettronica ordinaria o cosiddetta *normale* non può fornire.

2.1 Il documento informatico e il suo valore

"Il legislatore italiano ha ritenuto, fin dal 1997, di introdurre nel nostro ordinamento una definizione di documento informatico. L'operazione è stata ritenuta necessaria non tanto per ragioni tecnico-giuridiche, quanto piuttosto per abbattere un condizionamento culturale che porta a pensare il documento come necessariamente cartaceo, quando nulla obbliga in questo senso" [(29)].

La definizione di documento informatico è stata inserita all'art. 1 del D.P.R. 445/2000 e successivamente trasposta, esattamente identica, all'art. 1 comma 1 lettera p) del C.A.D.: "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*". Con il D.Lgs. 235/2010 è stata inoltre inserita, sempre nel CAD, all'art. 1 lettera p-bis), la definizione di documento analogico: "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*".

(29) Cit: G.FINOCCHIARO in *[12]*

E’ certamente condivisibile l’idea che un documento è *“una cosa che fa conoscere un fatto, in virtù del suo contenuto rappresentativo. In altri termini, ogni fatto può essere documentalmente rappresentato, e ogni documento deve rappresentare un fatto o un atto; un documento è una rappresentazione di uno stato di cose, non intesa come una mera attitudine psicologica, ma come il prodotto di un processo di riferimento linguistico. Nel mondo delle ICT, seguendo la definizione che ho proposta, un file è un documento nel momento in cui rappresenta uno stato di cose, indipendentemente dalla sua forma (il file può essere di testo, sonoro o video) e dal suo formato”* [(30)].

Resta in ogni caso la certezza che, dal punto di vista giuridico, un documento è destinato a produrre effetti diversi a seconda dei requisiti di forma che possiede.

Il documento cartaceo, debitamente sottoscritto, presenta caratteristiche tali da renderne difficile l’alterazione del contenuto, considerando quelli che sono i suoi elementi fondanti: la forma scritta od orale, di cui quella *scritta* rappresenta una attività

di documentazione; l’*imputabilità*, ossia la paternità dell’ atto che si realizza con la sottoscrizione, consentendo la riconducibilità ad un determinato soggetto; l’*integrità*, vale a dire la purezza dell’atto esente da alterazioni; questa è sempre verificabile ex post attraverso la materialità del supporto che fissa in maniera indelebile i segni grafici[(31)].

Tralasciando per un momento le questioni dell’imputabilità, dell’integrità e di qualsivoglia metodo di sottoscrizione, occorre differenziare, innanzitutto, il documento informatico da quello analogico sulla base della forma. La forma è la sembianza di un atto che, nel diritto, si sottopone alla valutazione normativa che lo sussume, la forma costituisce cioè le modalità con cui l’atto deve esteriorizzarsi ai fini della propria rilevanza giuridica.

---

(30) Cit: A.ROSSETTI, pag. 3 in *[13]*

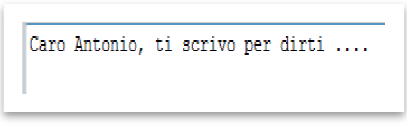
(31) Rif: M.MILANESE in *[14]*

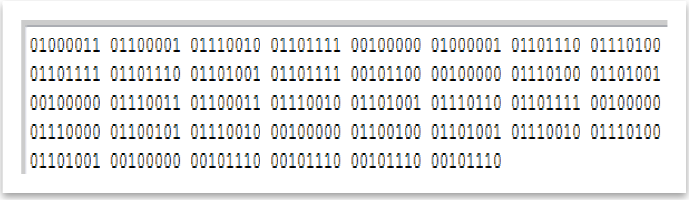
Il documento informatico è qualcosa di molto diverso dal documento cartaceo: è un *file*, cioè un contenitore di informazione digitalizzata: un agglomerato di dati che può essere manipolato, non solo come un'unica entità, ma anche nelle sue microcomponenti contenutistiche: tecnicamente i files non sono altro che insiemi ordinati di byte, cioè sequenze di semplici numeri binari, con un'evidente distinzione tra rappresentazione e contenuto[(32)]: distinzione che nel documento cartaceo non esiste.

Una considerazione generale, della quale necessariamente il legislatore ha dovuto tener conto, è che non costituiscono documenti informatici gli atti per i quali il computer è utilizzato come semplice dispositivo di produzione di stampa, al posto delle vecchie macchine da scrivere, in quanto il documento nasce con *"l'impressione dei segni grafici sulla carta, alla cui conservazione è affidata la conservazione dei significati"*[(33)]. Lo stesso vale per gli atti della pubblica amministrazione redatti con software di editing e nei quali la firma autografa è sostituita (con riferimento all'art. 3 del D.Lgs. 39/1993) dall'indicazione a stampa, nel documento prodotto, del nominativo del soggetto responsabile. Si tratta, in questi casi, non di documenti informatici ma di *normali* documenti cartacei prodotti con strumenti informatici. Se invece gli atti, nei quali i segni che vengono in considerazione non sono quelli impressi sulla carta, ma quelli direttamente registrati nella memoria del computer o su supporti informatici esterni e trasmissibili, il documento è dato direttamente dall'evidenza informatica, cioè dal file prodotto, ed è a tale realtà, squisitamente ed esclusivamente elettronica, che si ha riguardo quando si parla di documento informatico, tanto che rispetto ad essa, l'eventuale stampa su carta costituirebbe copia cartacea di originale informatico [(34)].

---

(32) Un file: evidenti le differenze tra una possibile rappresentazione e il contenuto:





(33) Cit: G.DI BENEDETTO, pag. 323 in *[16]*

(34) Rif: G.DI BENEDETTO, pag. 323 e ss. in *[16]*

La rilevanza giuridica di un file è tuttavia da intendersi al di là di qualunque sottoscrizione: i documenti informatici rilevano in quanto tali, in senso *oggettivo* indipendentemente dalla provenienza e dall'imputabilità ad un autore, prescindendo sostanzialmente dall'elemento *soggettivo*[(35)].

La loro efficacia probatoria è la medesima prevista per le riproduzioni meccaniche di cui all'art. 2712 c.c.: *"Le riproduzioni fotografiche o cinematografiche, le registrazioni fotografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime"*. Per sciogliere qualunque dubbio, l'art. 2712 è stato modificato dall'art. 23-quater del C.A.D. (così come disposto dall'art. 16 del D.Lgs. n. 235/2010) che inserisce la parola "*informatiche*" dopo le "*riproduzioni fotografiche*".

La valenza giuridica attribuita ai documenti informatici privi di qualsivoglia sottoscrizione, è stata più volte confermata in giurisprudenza. Si ricorda a tal fine la sentenza della Corte di Cassazione n. 11445 del 6 settembre 2001 dove, in tema di licenziamento per giusta causa, si evidenzia che i dati, forniti da un sistema computerizzato di rilevazione e documentazione, possono costituire, ai sensi degli artt. 2712 c.c. e 5 comma 2 del D.P.R. 513/1997, prova del fatto contestato se ne sia accertata la funzionalità del sistema informatico e le risultanze di esso possano costituire prova presuntiva congiuntamente a circostanze esterne ad esso, altrimenti provate[(36)]. In caso di disconoscimento, sarebbe lecito pensare che ciò possa far venir meno qualunque efficacia probatoria: non è opinione né della dottrina né della giurisprudenza, *"per le quali esse non sono rigidamente subordinate alla circostanza che colui contro il quale sono prodotte non le disconosca: al giudice non è preclusa la*

---

(35) Rif: M.MINERVA in *[17]*

(36) *"Questa Corte ha più volte ritenuto corrette le decisioni di giudici di merito, affermative della legittimità del licenziamento disciplinare di lavoratori dipendenti, che presupponevano, in maniera espressa o implicita, la questione della valenza probatoria di sistemi informatici (Cass. 24 maggio 1999 n. 5042 e Cass. 11 febbraio 2000 n. 1558), relative ad esattori della società Autostrade, per inadempienze accertate con le registrazioni informatiche; (Cass. 20 gennaio 1998 n. 476, in tema di inadempienze di dipendente bancario risultanti dal sistema informatico). In tali occasioni questa Corte ha ribadito il proprio insegnamento secondo cui la prova per presunzioni è dalla legge considerata come prova completa, ed è utilizzabile anche per considerare assolto l'onere probatorio in tema di motivi del licenziamento, sempre che sia fondata su un fatto notorio ovvero acquisito alla causa con i normali mezzi istruttori"*. (Estratto da Sentenza Cassazione Sezione Lavoro n. 11445 del 6.9.2001.
Rif: *http://www.legge-e-giustizia.it/index.php?option=com_content&task=view&id=2347&Itemid=131*)

possibilità di utilizzare liberamente il documento, apprezzandone l'attendibilità per formulare il proprio convincimento"[37]. Un documento informatico disconosciuto, che ha perso cioè il suo pieno valore probatorio, conserva tuttavia il minor valore di un semplice elemento di prova, che può essere integrato da ulteriori elementi. Inoltre, si ricorda che in alcune sentenze, tra cui si cita la n. 9884 dell'11 maggio 2005, la Corte di Cassazione ha stabilito che non basta invocare la natura genericamente *insicura* delle riproduzioni meccaniche per disconoscere una prova di natura informatica: occorre che il disconoscimento sia circostanziato ed inerente alla capacità rappresentativa della realtà e la genuinità e attendibilità del documento in questione e del suo contenuto[38].

E' possibile quindi rilevare una generale equiparazione del documento informatico al documento cartaceo, a tal fine vale ricordare quanto disposto dall'art. 20 comma 1 del C.A.D.: *"il documento informatico da chiunque formato nonché la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge"* ed al comma 1-bis: *"L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità";* in sostanza, se il documento è riconosciuto, fa piena prova, mentre se è disconosciuto può egualmente costituire prova se il giudice gli riconosce caratteristiche di sufficiente qualità, sicurezza integrità ed immodificabilità.

---

(37) Cit: A.FALZEA, P.GROSSI, E.CHELI, U.BRECCIA, pag. 641 in *[19]*

(38) Cassazione Civile Sez. Lav., Sentenza 11.05.2005 n. 9884:
"Nel caso in esame, il ricorrente impugnava la decisione della Corte d'appello di Roma con la quale era stata confermata, per quanto rileva in questa sede, l'efficacia probatoria dei tabulati prodotti in giudizio, in relazione ai quali il ricorrente non aveva disconosciuto la conformità ai fatti rappresentati. In particolare, il ricorrente lamentava che le risultanze di qualsivoglia sistema informatico possono essere alterate e adduceva la mancanza della prova del fatto che i tabulati prodotti in giudizio fossero quelli elaborati dalla macchina nel momento stesso in cui i fatti accadevano. Già la Corte d'appello rilevava che la contestazione era del tutto generica ed era consistita soprattutto nel paventare la possibile manomissione del sistema informatico. La Cassazione ritiene che i rilievi appaiono del tutto generici nel contenuto e ai fini specifici dell'oggetto della contestazione, non riguardando la specifica conformità dei dati ai fatti ed alle cose rappresentate, non decisivi. La Cassazione dunque conferma l'efficacia probatoria dei tabulati prodotti attraverso il sistema informatico, non essendo stato effettuato il disconoscimento o essendo stato effettuato in modo del tutto generico. Con l'occasione la Corte ribadisce che la contestazione esclude la piena efficacia probatoria della riproduzione meccanica 'ove abbia per oggetto il rapporto di corrispondenza fra la realtà storica e la riproduzione meccanica' e aggiunge che ove la contestazione con questo specifico contenuto vi sia stata, la riproduzione, pur perdendo il suo pieno valore probatorio, conserva il minor valore di un semplice elemento di prova, che può essere integrato da ulteriori elementi". Cit: G.FINOCCHIARO in *[24]*

In merito alla sottoscrizione, il legislatore italiano, al fine di poter in qualche misura parificare il documento informatico a quello cartaceo, ha introdotto la normativa relativa alla firma digitale già con il D.P.R. 513/97 *("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2°, della legge 15 marzo 1997, n. 59").*

La Direttiva comunitaria 1999/93/Ce per la costituzione di un quadro comunitario per le firme elettroniche, attuata in Italia con il D.Lgs. 10/2002, ha riconosciuto valore giuridico alle firme elettroniche, oltre che alla firma digitale. Successivamente è stato emanato il D.P.R. 137/2003 *("Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'art. 13 del decreto legislativo 23 gennaio 2002, n. 10")* con lo scopo di coordinare le disposizioni della legislazione italiana in tema di documento informatico e di firma digitale con quelle di derivazione comunitaria sulla firma elettronica. Il C.A.D. e le sue successive modificazioni in materia di firme elettroniche, effettuate attraverso il D.Lgs. 159/2006 e il D.Lg.s. n. 235/2010, ha riordinato e consolidato la normativa previgente.

La firma autografa e le firme elettroniche, pur avvalendosi dello stesso termine "firma", hanno natura molto diversa, la prima costituisce il risultato di un gesto umano mentre la seconda è il risultato di una procedura tecnologica: *"L'utilizzo del medesimo termine è foriero di conseguenze rilevanti sul piano della rappresentazione della conoscenza. Conduce ad associare naturalmente, quasi istintivamente, i due oggetti e a considerarli realtà assimilabili e quindi, in questo caso, sottoposti al medesimo regime giuridico"* [(39)].

Considerando la questione da un punto di vista pratico, potremmo dire che nelle sottoscrizioni cartacee, la "chiave" per apporre la firma si risolve in qualcosa che ci offre il segno di quel che *una persona è*: riusciamo a risalire ad una determinata persona perché la firma è il risultato delle sue caratteristiche psicofisiche (che è l'analogo meccanismo utilizzato per le firme elettroniche basate su caratteristiche come la retina o l'impronta digitale).

---

(39) Cit: G.FINOCCHIARO in *[20]*

Altri sistemi potrebbero essere basati su segni che ci dicono quel che *una persona sa* (come una parola chiave o un codice) e altri ancora su quel che *una persona ha* (come tessere magnetiche, ecc...) [(40)].

Il legislatore ha disposto all'art. 1 del C.A.D. le seguenti tipologie di firme elettroniche:

- firma elettronica: "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*", non essendo specificata alcuna tecnologia, può trattarsi di una password, di una firma autografa digitalizzata tramite scanner, così come di una firma biometrica.

- firma elettronica avanzata: "*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*", può trattarsi di "One Time Password", di firma autografa su tablet o di firma biometrica, verificate le caratteristiche e verificato il contesto, anche procedurale, in cui la firma è inserita e le proprietà del documento[(41)].

- firma elettronica qualificata: *"un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato*[(42)] *e realizzata mediante un dispositivo sicuro per la creazione della firma"*.

---

(40) Rif: G.DI BENEDETTO, pag. 326 in *[16]*

(41) Rif: G.FINOCCHIARO in *[20]*

(42) Il certificato qualificato è un certificato elettronico, che collega l'identità del titolare ai dati utilizzati per verificare la firma elettronica, che deve essere conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, in particolare i certificati qualificati devono includere:

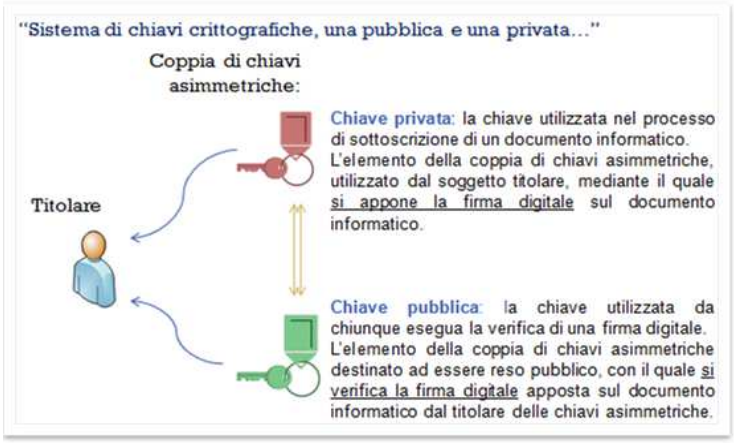
a. l'indicazione che il certificato rilasciato è un certificato qualificato;
b. l'identificazione e lo Stato nel quale è stabilito il prestatore di servizi di certificazione;
c. il nome del firmatario del certificato o uno pseudonimo identificato come tale;
d. l'indicazione di un attributo specifico del firmatario, se il certificato ha uno scopo specifico;
e. i dati per la verifica della firma corrispondenti ai dati per la creazione della firma sotto il controllo del firmatario;
f. un'indicazione dell'inizio e del termine del periodo di validità del certificato;
g. il codice d'identificazione del certificato;
h. la firma elettronica avanzata del prestatore di servizi di certificazione che ha rilasciato il certificato;
i. i limiti d'uso del certificato, ove applicabili;
j. i limiti del valore dei negozi per i quali il certificato può essere usato, ove applicabili.

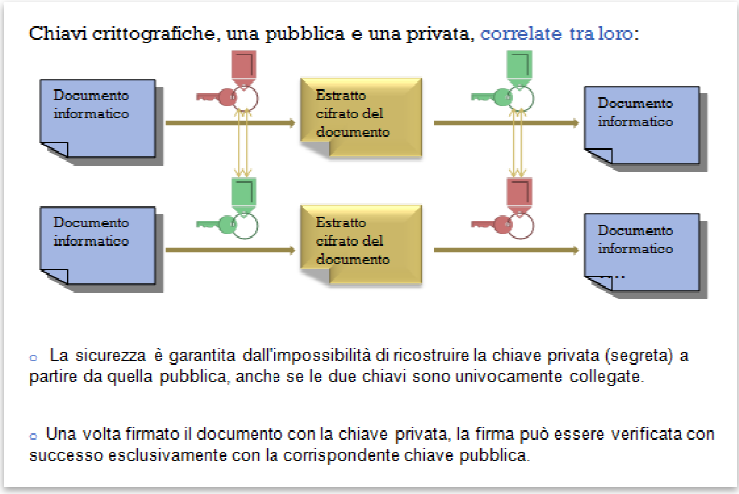
- firma digitale: *"un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche*[(43)]*, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"*;

All'art. 21 del C.A.D. si dettano disposizioni in materia di valore probatorio dei documenti informatici con firma elettronica:

- al comma 1: *"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"*.

(43) La firma digitale è basata su due chiavi cioè due codici tra loro strettamente correlati:





- al comma 2: *"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 c.c.. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria"*.
- al comma 2-bis): *"Salvo quanto previsto dall'art. 25 (in materia di firma autenticata), le scritture private di cui all'art. 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'art. 1350, numero 13, del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.*

Senza intenzione di voler trattare in maniera dettagliata le caratteristiche delle diverse tipologie di firme elettroniche, in questo scritto preme unicamente evidenziare come il legislatore abbia ben distinto il valore giuridico di un documento informatico a seconda del tipo di firma elettronica ad esso associata. La giurisprudenza si è più volte pronunciata su questioni giuridiche di rilievo come ad esempio l'estromissione da gare per appalti pubblici o stipula di contratti attraverso procedure telematiche[(44)].

[(44)] In merito si citano due sentenze da F.NOVARIO, pag 12 in *[18]:*

- Tar Puglia, Bari, 24.5.2012, n. 1019:

Invero, la P. s.r.l. è stata legittimamente esclusa dalla procedura telematica di gara oggetto della presente controversia per aver omesso di sottoscrivere la propria offerta trasmessa in via telematica, avendo utilizzato uno strumento (inserimento del codice PIN presso l'apposita piattaforma informatica del sito internet *www.albofornitori.it* gestito da CSAMED s.r.l.) che non assicura certezza in ordine alla provenienza del documento. Ai sensi dell'art. 77, comma 6, lett. B) del D.Lgs. n. 163/2006, le offerte presentate per via telematica possono essere effettuate solo utilizzando la firma elettronica digitale come definita e disciplinata dal D.Lgs. n. 82/2005.

- Tar Friuli Venezia Giulia, Trieste, 15.12.2011, n. 564:

La situazione di fatto verificatasi in concreto e cioè la stipulazione del contratto di fideiussione per via telematica con conseguente firma digitale del fideiussore e trasmissione in allegato all'offerta della copia cartacea dello stesso senza che la firma del garante, apposta per via telematica e quindi senza sottoscrizione del cartaceo, risultasse autenticata da pubblico ufficiale non si può assimilare ad una ipotesi di inesistenza del contratto di fideiussione. Infatti il contratto esiste dal momento del perfezionamento dell'accordo con l'apposizione della firma in via digitale e nemmeno dagli artt. 23 e 25 D.Lgs. n. 82/2005 si può in qualche modo inferire l'inesistenza del contratto firmato in via digitale ma riprodotto su carta senza l'autentica della firma digitale.

2.2 Il valore di una e-mail

Molto tempo è passato dall'invio della prima mail[45] tuttavia da allora qualcosa non è cambiato: il dubbio che la mail sia arrivata o meno a destinazione, quando scriviamo ad un indirizzo di posta elettronica per noi inconsueto, ancora ci accompagna.

I gestori di posta elettronica[46], che molto spesso ci forniscono il servizio gratuitamente, anche se non sono tenuti a farlo, potranno segnalarci che l'indirizzo del destinatario non esiste, che la sua casella è piena, ecc.[47].

---

[45] Ray Tomlinson, ingegnere informatico (che lavorava presso la Bolt Beranek & Newman, l'azienda che nel 1968 aveva vinto l'appalto per lo sviluppo della rete Arpanet per il Dipartimento della Difesa statunitense), inviò il primo messaggio e-mail nel 1972 tra due calcolatori della sede di Cambridge, il cui contenuto fu QWERTYUIOP, la riga alfabetica superiore della tastiera di una macchina per scrivere americana. A Tomlinson è anche attribuita la scelta della caratteristica @ per identificare gli indirizzi e-mail, anche se il primo utilizzo del simbolo è da far risalire ai mercanti veneziani del Cinquecento, che utilizzavano la @ come abbreviazione commerciale per *anfora*. Quest'ultima era l'unità per le misure di peso e capacità dalle origini antichissime – diffusa anche nel mondo arabo-ispanico e in quello greco-latino – equivalente a poco più di 18 litri. (Mario Grasso e Valentino Laurenzi, pag.152 in *Da @ a Zorch. Storia, parole, date, luoghi e protagonisti del Web che i manager devono conoscere*, FrancoAngeli, 2001)

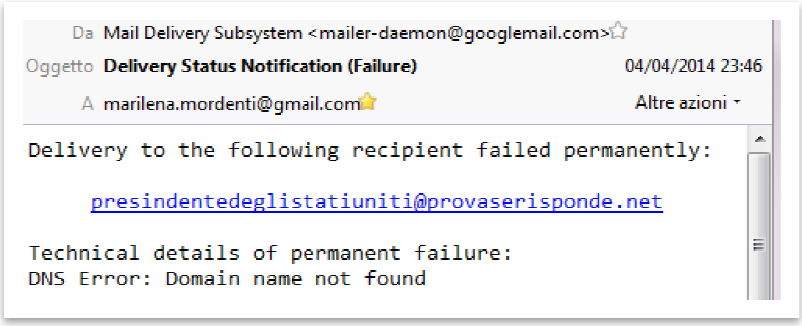
[46] La classifica dei Mail Server gratuiti più utilizzati:

1) Gmail - Free Email Service
2) Zoho Mail - Free Email Service
3) AIM Mail - Free Email Service
4) iCloud Mail - Free Email Service
5) Outlook.com - Free Email Service
6) Yahoo! Mail - Free Email Service
7) Mail.com and GMX Mail - Free Email Services
8) Shortmail - Free Email Service
9) Inbox.com - Free Email Service
10) Facebook Messages - Free Email Service
11) My Way Mail - Free Email Service

(Rif: Rilevazione a febbraio 2014 da *http://email.about.com/od/freeemailreviews/tp/free_email.htm*)

[47] Qui sono riportati due esempi di risposte da un Mail Server a fronte dell'invio di una e-mail ad indirizzi di posta elettronica inesistenti.

- Il dominio al quale ho scritto (*provaserisponde.net*) non esiste:

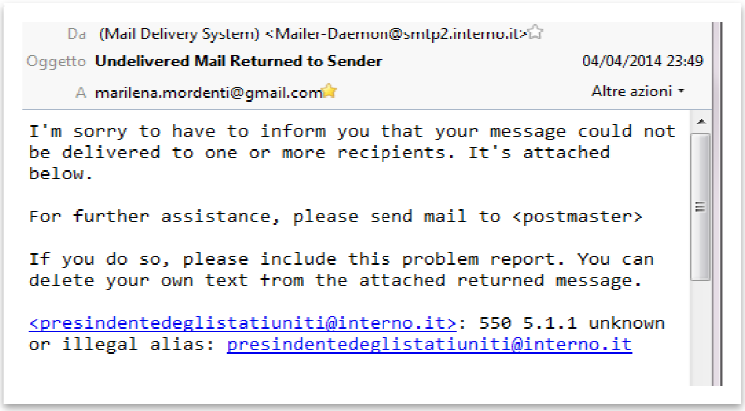


(segue in [47-bis])

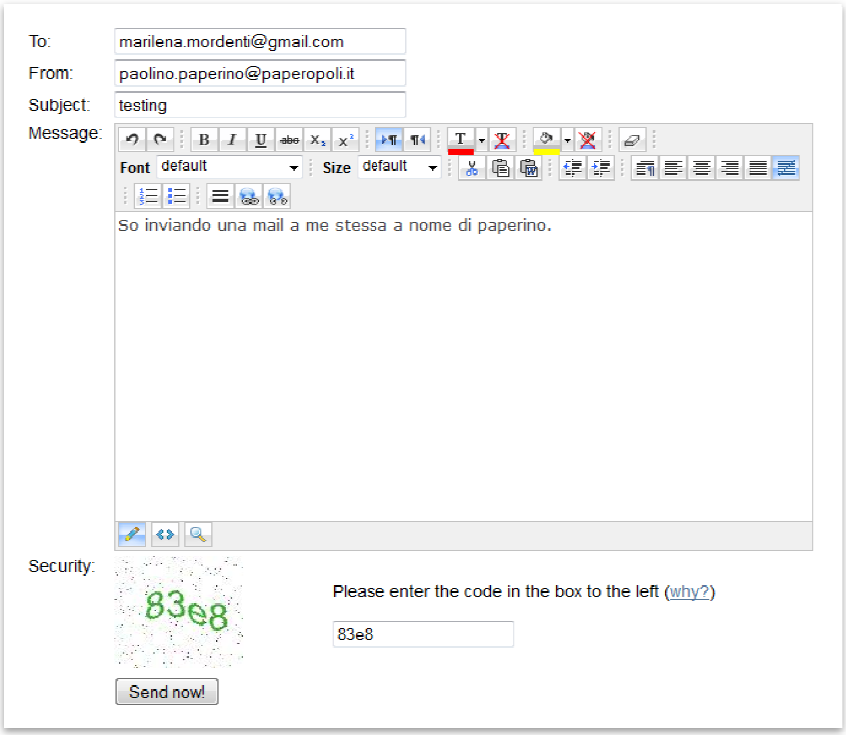
Normalmente, se il nostro servizio di posta elettronica lo consente, chiediamo la ricevuta di lettura; sta tuttavia al destinatario dell'e-mail, aprendola, decidere se inviarci o meno la conferma di aver letto il messaggio.

Inoltre possono subentrare incertezze anche sulla provenienza di una e-mail ricevuta, in quanto esistono servizi gratuiti che consentono di anonimizzare l'indirizzo e-mail del mittente o di "inventarlo"[48].

(47-bis) - Qui invece non esiste la casella *presidentedeglistatiuniti* nel dominio *interno.it*:



(48) Qui sotto un esempio: collegandomi ad un sito che consente di anonimizzare il mittente, ho inviato a me stessa una e-mail proveniente da un indirizzo inesistente:

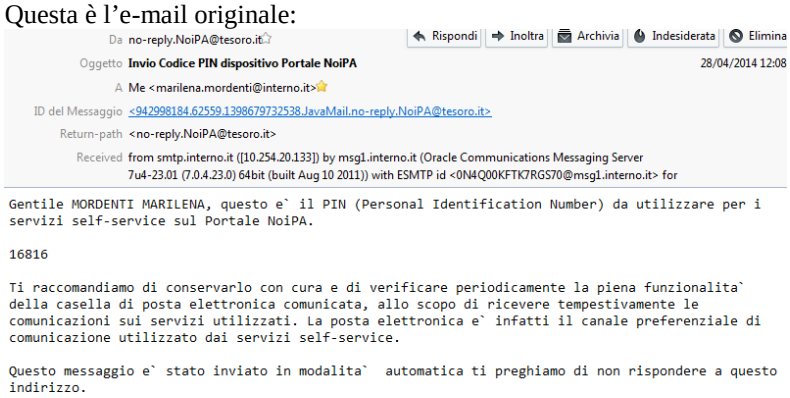


e l'e-mail è regolarmente arrivata nella mia casella.

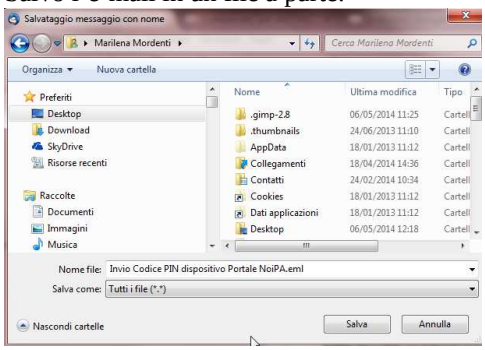
Altri dubbi possono infine subentrare sui contenuti trasmessi e/o ricevuti, ad esempio alcuni client di posta elettronica consentono di modificare successivamente ed in maniera agevole il contenuto delle mail inviate o ricevute[49].

[49] Un esempio di modifica del contenuto di una mail ricevuta su un client di posta elettronica.

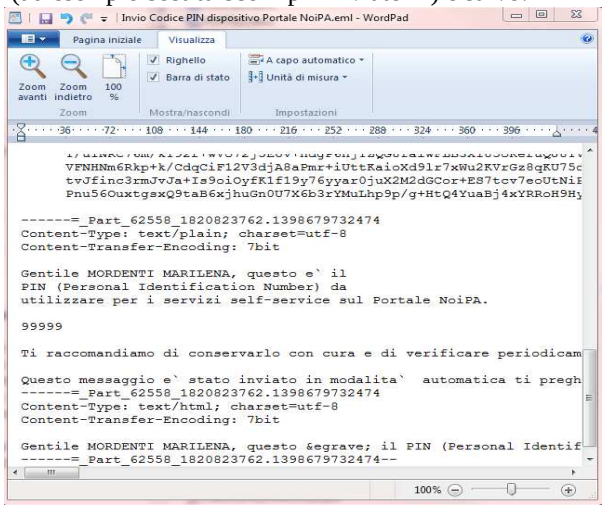
Questa è l'e-mail originale:



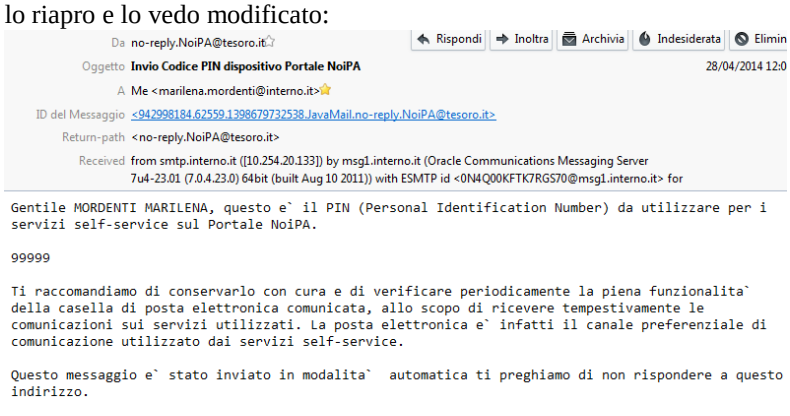
Salvo l'e-mail in un file a parte:



Poi ne modifico il contenuto con un gestore di testi (ad esempio sostituisco il pin inviatomi) e salvo:



Infine cancello l' e-mail originale e trascino il file modificato tra la posta in arrivo, lo riapro e lo vedo modificato:

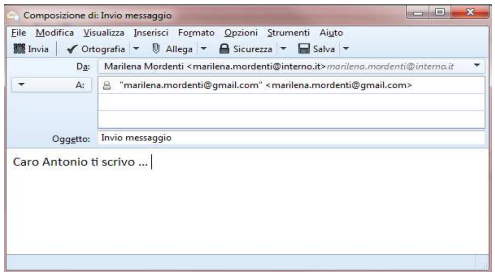


Stanti le incertezze fino a qui riportate, possiamo tuttavia affermare che l'e-mail non solo è un documento informatico, ma un documento informatico dotato di una firma elettronica.

La firma elettronica è costituita dall'insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. Il C.A.D., all'art. 1 lettera u-ter) fornisce puntuale definizione di identificazione informatica: *"la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso"*. Nell'utilizzo della posta elettronica sussiste certamente l'associazione logica tra le credenziali che utilizziamo per aprire la casella e il suo contenuto: per accedere alla casella di posta normalmente apriamo la pagina web del nostro Server Mail e accediamo al sistema informatico digitando *ciò che noi sappiamo*, cioè l'indirizzo della nostra casella e la password. Avvenuta l'autorizzazione all'accesso da parte del Server, possiamo inviare un'e-mail: il software che ci supporta incaselerà ciò che noi scriviamo in una struttura, o meglio, produrrà un testo seguendo un rigido formalismo(50) necessariamente noto e condiviso tra i server di posta pubblici in internet al fine di consentire il raggiungimento del destinatario(51).

(50) Lo standard mondiale di riferimento per la struttura e la notazione sintattica dei messaggi di posta elettronica è l'RFC (Request for Comments) 2822, la cui pubblicazione è cura dell'Internet Engineering Task Force (IETF). (Rif: *http://tools.ietf.org/html/rfc2822*).

(51) Inviamo una mail:



Questo è ciò che viene trasmesso:

In una e-mail, il testo che inviamo è sempre preceduto dagli *headers* che identificano le informazioni di instradamento del messaggio, incluso mittente, destinatario, data e oggetto. Alcune di queste intestazioni sono obbligatorie come: *From*, *To* e *Date*; altre sono facoltative, ma consuetamente utilizzate, come l'oggetto, *Cc* (carbon copy) e *Bcc* (blind carbon copy). Tra gli headers sono presenti inoltre i nomi e gli *indirizzi ip* (internet protocol) dei dispositivi di rete che vengono attraversati, prima che l'e-mail sia a disposizione sul Server Mail del nostro destinatario, insieme ai diversi *timestamp*, cioè data e ora in cui il messaggio attraversa i diversi dispositivi. Ciò comporta indubbiamente che, insieme al documento informatico, cioè a ciò che noi scriviamo nell'e-mail, *"viaggiano"* - e quindi sono allegati - anche altri dati in forma elettronica, necessari certamente al raggiungimento del destinatario, ma ovviamente connessi logicamente alla nostra iniziale identificazione informatica(52).

Stanti le peculiarità tecniche, si può ritenere condivisibile che il nostro legislatore abbia quindi disposto la categoria di firma elettronica "*prescindendo dalla*

(52) Questo è ciò che il destinatario riceve:

```
Delivered-To: marilena.mordenti@gmail.com
Received: by 10.217.126.202 with SMTP id dn52csp321689web;
        Thu, 20 Mar 2014 10:18:37 -0700 (PDT)
X-Received: by 10.14.37.8 with SMTP id x8mr43056627eea.32.1395335917546;
        Thu, 20 Mar 2014 10:18:37 -0700 (PDT)
Return-Path: <marilena.mordenti@interno.it>
Received: from smtp1.interno.it (mailout.interno.it. [62.77.42.102])
        by mx.google.com with ESMTP id x41si3911476eee.132.2014.03.20.10.18.37
        for <marilena.mordenti@gmail.com>;
        Thu, 20 Mar 2014 10:18:37 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of
marilena.mordenti@interno.it designates 62.77.42.102 as permitted sender) client-
ip=62.77.42.102;
Authentication-Results: mx.google.com;
       spf=pass (google.com: best guess record for domain of marilena.mordenti@interno.it
designates 62.77.42.102 as permitted sender) smtp.mail=marilena.mordenti@interno.it
X-AuditID: 0afe14c5-b7f558e000005342-f7-532b22ed957a
Received: from posta.interno.it (Unknown_Domain [10.254.20.37])
        by smtp1.interno.it (SMTP Server) with SMTP id 75.DC.21314.DE22B235; Thu, 20 Mar
2014 18:18:37 +0100 (CET)
Received: from [127.0.0.1] ([10.54.4.196]) by mta1.interno.it (1.0)
 with ESMTPPSA id <0N2Q006LBW308770@mta.interno.it> for
 marilena.mordenti@gmail.com; Thu, 20 Mar 2014 18:18:42 +0100 (MET)
Message-id: <532B2307.5020505@interno.it>
Date: Thu, 20 Mar 2014 18:19:03 +0100
From: Marilena Mordenti <marilena.mordenti@interno.it>
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101
 Thunderbird/24.4.0
MIME-version: 1.0
To: "marilena.mordenti@gmail.com" <marilena.mordenti@gmail.com>
Subject: Invio messaggio
Content-type: text/plain; charset=ISO-8859-15; format=flowed
Content-transfer-encoding: 7bit
X-Brightmail-Tracker:
H4sIAAAAAAAAA12Qe0xTZxjG+dpzTr82nHE4FHztWDQnXCbOC96ybGaazG0mRkJSTQzR6DEc
        aLfe7CmkNTFB6zIkQZiVuJVRSsSEi4rSKmwmVDqJ6NxQx9QqVo1/4AUv3JImRN05rczO/558
        v+d5v/d9sJJtUumw0eIQ7BbexFEaQvNam7voGbdQv3R/ddqnAe9Tci1a/6v3rqoYlWhWlwom
        Y6VgX/LFDo3B195C2rKdwaHnVBXKqkEYA7MCrg6ra5BakllwNdpF1SANZpnjCIaae5AMWKYf
        wfhovqxpZgFEZn6PvxNMLlQFJg1ZU8wqaNrXR8k6k9kK7b0XFAl/OsQ80bhHy6yB6P1BUtYZ
        DMBYZJqUd1Ayq6G/uUx+VjLzIHD8mbIe0d6ktPedy5vk8iNlB2JEs8NWuDhRiHWx0dGNEp0M
        9KKorzCMGIy4VNqpXqhnSb5SdJnDaCVWcDq6Cefo2Yyd1lKXgRcN28WKnWajKBqtFi6THsuW
        7B/8x+wVJkEMI8BKTkvvmi8xupR37Rbs1ln0ISa4ObTLqtKzTDnvEL4TBJtgn6WfY8x9RKOU
        lBQ2yy6UC84yo0naN/lPoHvkuenJ+G1agdVhtBynCnMTI1jRxptFY3lyXEtPxdeaRfHoZfQl
        vj3cuVfBEharRdBl0wcaCvRspmwyVFj+v4FuDv2nPIJJovEpT9A0kjoE2icXli41/d7fGYlg
        6lsSDy3rlzLMZxCKXNsIff7Dm6H+ym97IBiL/oDAM/2mE0HgUGcQQbB58hyC4RZfCEFXyH9e
        0qMTUtW+6iu3EBx6OOhWwK3Ig+8VMPXjwR4lxMb21xLwd2uoi4A3Ye9fBATCA0MEjMR6XxBw
        2j0ZJOHRTFM/CW2XakdIOPWw7jEJg5EGNwXX++pbKJiqdQcpaDs9U6eC676RRlV8ExVcG6g6
        i+Hi7cONahhtqPWrn0ilK96V7uDfP1xLp8l90rMofrmuCuUexa7zJ21nuk/dyK872brlp7y1
        Szjr89a2knHWc49Km39igaf+aNGBiYb1JXmL3Navf972ldN8sTS9aLc670XOJ5s23G/cdDNy
        5J+Pd3le3jl2sNtflv9LQWTiW6rjj7b8E6biV86SnDXnLgS/ic2N2ZYZKm3b7TGq+ub4uh25
        dwrnhThCNPCFBUq7yP8LQ3fnlzAEAAA=

Caro Antonio ti scrivo ...
```

tecnica utilizzata per creare l'associazione del documento al suo titolare e questo con la precisa intenzione di lasciare ampia libertà nel commercio elettronico tra privati (in modo che si possano trovare nel tempo anche nuove soluzioni tecnologiche più appropriate alle esigenze della prassi commerciale). In questo modo possono rientrare tra i documenti firmati elettronicamente tutti quei documenti che permettano, in maniera più o meno sicura, l'associazione del documento ad un soggetto: tra questi rientra certamente l'e-mail!"[(53)].

Diversi pronunciamenti giurisprudenziali hanno confermato l'applicazione del disposto del primo comma dell'art. 21 del C.A.D.. Si ricordano in tal senso due sentenze: la prima del Tribunale di Cuneo nel 2003[(54)], dove si rileva che una specifica e-mail possa costituire, a tutti gli effetti, una promessa unilaterale di pagamento e/o una ricognizione di debito in forma di scrittura privata, e la seconda del Tribunale di Prato nel 2011[(55)], con riferimento ad una e-mail volta a provare l'avvenuta tempestiva denuncia dei vizi della merce acquistata.

---

(53) Cit: A.LISI in *[21]*

(54) La società BB s.r.l., debitrice nei confronti della AA s.r.l. della complessiva somma di € 2.593,36 per alcune prestazioni e forniture, con una e-mail del 20.10.2003, in risposta alla lettera di diffida del legale della società AA s.r.l., assicura il pagamento di quanto dovuto entro 10 giorni. Nonostante quanto promesso e i ripetuti solleciti, la società BB s.r.l. non provvedeva al pagamento costringendo la società AA s.r.l. al recupero forzato del credito. Facendo proprie le argomentazioni di parte ricorrente, il giudice ha ritenuto che la e-mail del 20.10.2003 costituisse a tutti gli effetti una promessa unilaterale di pagamento e/o una ricognizione di debito in forma di scrittura privata. Il messaggio di posta elettronica costituisce un documento informatico sottoscritto con firma elettronica c.d. "semplice", ai sensi degli artt. 1, comma 1, lett. b), 8 e 10, comma 2, del T.U. 445/2000 e successive modificazioni, dal momento che il mittente per poter creare e inviare detta e-mail, deve eseguire un'operazione di validazione inserendo user-id e password, in quanto tale la e-mail soddisfa il requisito legale della forma scritta richiesto dall'art. 634 c.p.c. per la concessione del decreto ingiuntivo. (Tribunale di Cuneo, decreto ingiuntivo n. 848/03 del 15.12.2003). Rif: L.TURINI in *[22]*

(55) Secondo il Tribunale di Prato (15.4.2011), l'email inviata in assenza di un meccanismo di posta elettronica certificata non consente di identificare in maniera univoca il mittente, né di provare la ricezione del messaggio da parte del destinatario. Tuttavia, è indubbio che l'email possa essere qualificata come documento dotato di firma elettronica "dato che lo username e la password usati per l'accesso alla casella di posta elettronica integrano comunque un insieme di dati utilizzati come metodi di identificazione informatica ai sensi dell'art. 1, lett. q)" del CAD. Conseguentemente, l'efficacia probatoria dell'email è liberamente valutabile in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità e –aggiunge la sentenza– anche delle ulteriori risultanze processuali, in primo luogo il mancato disconoscimento e la tempestiva contestazione dei fatti ivi rappresentati. Nel caso di specie, il destinatario aveva sin da subito disconosciuto le vicende fatte valere a mezzo dell'email in questione e tale rilievo, mancando ulteriori elementi idonei a confermarne il contenuto, ha comportato una valutazione negativa sul piano probatorio. Le pretese dell'opponente sono state, dunque, rigettate. La decisione è comunque di grande rilevanza perché riafferma che l'email è un documento dotato di firma elettronica. Rif: B.SUCCI in *[23]*

L’e-mail è quindi, senza alcun dubbio, un documento informatico con firma elettronica, dal momento che le credenziali utilizzate, cioè indirizzo della casella e password, ne integrano la definizione di firma elettronica e la sua efficacia probatoria è liberamente valutabile in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2.3 L’e-mail certificata

La posta elettronica ordinaria, pur essendo uno strumento facilmente accessibile da qualsiasi utilizzatore, non fornisce piene garanzie di effettivo invio e consegna di un messaggio, certezza sulla sua paternità, sulla data e l’ora dell’invio, sulla coerenza e l’integrità di quanto spedito con quanto ricevuto e sull’effettiva ricezione. Per queste ragioni nasce la posta elettronica certificata che può essere impiegata in qualunque contesto ove sia necessario, o si desideri, disporre di uno strumento opponibile ai terzi che comprovi l’invio e la consegna di una e-mail.

Facendo un parallelo con la posta tradizionale, possiamo affermare che la posta elettronica sta alla lettera ordinaria come la posta elettronica certificata sta alla raccomandata, con due vantaggi in più:

- nella trasmissione via p.e.c. è certa la casella mittente e quindi il titolare, mentre non è tracciato colui che spedisce una raccomandata (posso fare una raccomandata in posta e indicare come mittente Paolino Paperino!);
- nella trasmissione via p.e.c. sussiste il legame certo ed opponibile della trasmissione con il documento trasmesso, tale possibilità è preclusa con la raccomandata (se inserisco un foglio bianco in una busta e invio una raccomandata … potrei affermare di aver spedito il documento che il mio destinatario attendeva...).

Vengono sostanzialmente superate le “debolezze” della posta elettronica ordinaria:

- certificazione della data e dell’ora di spedizione del messaggio e degli allegati;
- tracciabilità della casella mittente e quindi del suo titolare;
- certificazione della data e dell’ora di ricezione del messaggio e degli allegati;
- elevati requisiti di qualità e continuità del servizio;
- applicazione di procedure a garanzia della privacy e della sicurezza;

- archiviazione da parte del gestore di tutti gli eventi associati ad invii e ricezioni.

La definizione di posta elettronica certificata è presente all'art.1 lettera v-bis) del C.A.D.: *"un sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi"*. Tali ricevute, fornite in tempo reale al mittente, *"costituiscono la documentazione elettronica attestante l'invio e la consegna di documenti informatici"* come dispone l'art. 1 lettera g) del D.P.R. 68/2005.

La normativa generale sulla posta elettronica certificata nasce comunque nel contesto del più ampio progetto di informatizzazione degli uffici pubblici conosciuto come e-Government, e si presenta come un'innovazione capace di generare enormi risparmi sul piano economico nei settori pubblici e privati e al contempo di semplificare i rapporti tra privati e tra costoro e la pubblica amministrazione(56). Inoltre, in un Paese come l'Italia dove il diritto trae fondamento dalla legge scritta (c.d. *Civil Law*), si è ritenuto necessario definire puntualmente il formato delle ricevute e le caratteristiche tecniche di funzionamento, ed inoltre è stata introdotta e disciplinata la figura del gestore del servizio di posta elettronica certificata(57).

I soggetti coinvolti nella trasmissione di una e-mail p.e.c. sono: il *mittente*, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici, il *destinatario*, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici e il *gestore* (o i gestori se mittente e destinatario si affidano a due gestori diversi) del servizio.

(56) Rif: CASSANO e CIMINO, pag. 489 in *[25]*

(57) Rif: PETRUCCI, ORAZI, TORTORELLI in *[26]*

I gestori possono essere pubbliche amministrazioni o privati e sono inseriti in un elenco pubblico[58] a cura dell'Agenzia per l'Italia Digitale, essi amministrano uno o più domini di posta elettronica certificata[59].

I gestori si interfacciano con gli altri gestori garantendo l'interoperabilità[60] del proprio servizio (come disposto al comma 2 dell'art. 5 del D.P.R. 68/2005); essi devono aver presentato domanda di iscrizione all'elenco pubblico curato dall'Agenzia per l'Italia Digitale, secondo le modalità e nelle forme previste dalla Circolare CNIPA n. 56/2009 e, in particolare, devono fornire il manuale operativo che individua le regole generali, gli standard tecnologici di riferimento e le procedure seguite nello svolgimento della propria attività; tale manuale deve essere pubblicato a garanzia dell'affidabilità dei servizi offerti ai titolari di caselle di posta elettronica certificata e ai loro corrispondenti[61].

---

[58] L'elenco dei gestori di posta elettronica certificata è disponibile sul sito dell'Agenzia per l'Italia Digitale all'indirizzo: *http://www.agid.gov.it/infrastrutture-sicurezza/pec-elenco-gestori.*

[59] Un dominio di Posta Elettronica Certificata è un dominio DNS (Domain Name System) dedicato alle caselle di posta elettronica degli utenti di Posta Certificata. Un Domain Name System - DNS (sistema dei nomi a dominio) è un sistema impiegato per risolvere i nomi dei nodi di rete in Indirizzi IP. Il servizio è realizzato da un sistema di Data Base distribuiti: i server DNS, appunto. All'interno di un tale dominio le caselle di posta elettronica devono appartenere ad utenti di Posta Certificata. Rif: GAMBETTA in *[27]*

[60] I gestori utilizzano un server LDAP che costituisce la struttura tecnica relativa all'elenco pubblico dei gestori e contiene l'elenco dei domini e dei gestori con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute e delle buste di trasporto. L'interoperabilità tra i diversi gestori viene garantita, dal legislatore, attraverso la scelta di vincolarli all'utilizzo di specifici standard tecnologici definiti nell'art. 3 del Decreto Ministeriale 2 novembre 2005 e dettagliatamente specificati nell'allegato a detto D.M.:

a) RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);
b) RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
c) RFC 1912 (Common DNS Operational and Configuration Errors);
d) RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
e) RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5);
f) RFC 2633 (S/MIME Version 3 Message Specification);
g) RFC 2660 (The Secure HyperText Transfer Protocol);
h) RFC 2821 (Simple Mail Transfer Protocol);
i) RFC 2822 (Internet Message Format);
j) RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification);
k) RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
l) RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
m) RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)

[61] Il manuale operativo di ogni gestore p.e.c. viene mantenuto disponibile alla consultazione sul proprio sito. A titolo di esempio per il certificatore Telecom Italia Trust Technologies S.r.l. (già I.T. Telecom S.r.l.) è disponibile all'indirizzo *http://www.trusttechnologies.it/default.aspx?idPage=632.*

Coloro che vogliono diventare gestori devono rispettare i requisiti previsti dall'art. 14 del DPR. 68/2005 e, se non sono pubbliche amministrazioni, deve trattarsi di società di capitali a capitale sociale interamente versato non inferiore a un milione di euro. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere requisiti di onorabilità; dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio ed impiegare personale dotato di conoscenze specifiche e dimestichezza con procedure di sicurezza appropriate. Sono tenuti ad utilizzare la firma digitale per certificare le attività svolte e adottare adeguate misure per garantire l'integrità e la sicurezza del servizio. Devono prevedere servizi di emergenza che assicurino, in ogni caso, il completamento della trasmissione e disporre di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi. Infine sono tenuti ad effettuare test periodici per verificare l'interoperabilità dei propri sistemi e a comunicare tempestivamente eventuali malfunzionamenti, classificando i livelli di criticità rilevati. In caso di problemi significativi, l'Agenzia per l'Italia Digitale può predisporre la sospensione dell'attività ed effettuare sopralluoghi presso le strutture operative utilizzate dal gestore per verificare la conformità del sistema p.e.c. (come da Circolare CNIPA del 7 dicembre 2006, n. 51) [(62)]. Secondo l'art. 15 del D.P.R. 68/2005, possono esercitare il servizio di posta elettronica certificata anche gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea, in tal caso l'Agenzia per l'Italia Digitale ne verifica l'equivalenza e la rispondenza ai requisiti. Le pubbliche amministrazioni possono svolgere autonomamente attività di gestione del servizio p.e.c., oppure avvalersi dei servizi offerti da altri gestori pubblici o privati. Se le P.A. decidono di divenire gestori, esse possono rilasciare caselle p.e.c. ai privati ma tali caselle sono valide limitatamente alle trasmissioni tra le amministrazioni medesime ed ai privati cui sono rilasciate. In ogni caso le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.

In merito all'identità dei fruitori del servizio di posta elettronica certificata, cioè ai titolari, fermo restando che il servizio deve essere fornito conformemente a quanto previsto dal D.Lgs. n. 196/2003 in materia di protezione dei dati personali, occorre

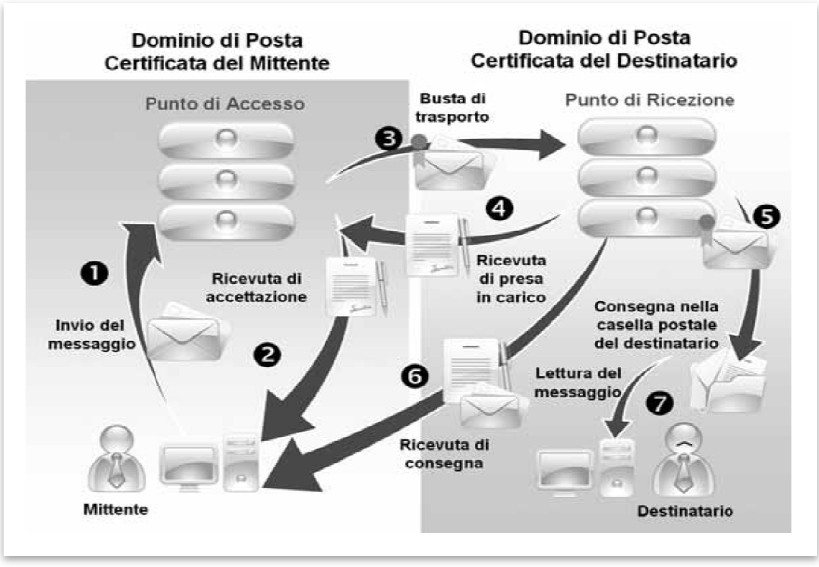
[(62)] Rif: Agenzia per l'Italia Digitale (*http://www.agid.gov.it/infrastrutture-sicurezza/posta-elettronica-certificata*)

ricordare che l'utilizzo della posta certificata garantisce l'identità della casella mittente in quanto è assicurata l'inalterabilità dell'indirizzo associato alla casella dalla quale si effettua l'invio del messaggio. Inoltre la p.e.c. è in grado di garantire l'associazione fra il titolare del servizio e la relativa casella in quanto, il soggetto che intende richiedere il servizio, deve presentare al gestore anche un documento che attesti la sua identità[63].

2.4 Le ricevute di accettazione e consegna

Il documento informatico, trasmesso per via telematica, si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore (art. 45 comma 2 del C.A.D.). La validità della trasmissione e ricezione del messaggio di posta elettronica certificata sono attestate rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna fornite dal gestore (art. 4 comma 6 del D.P.R. 68/2005).

Si descriverà ora in dettaglio l'invio di una e-mail da una casella di posta elettronica certificata ad un'altra casella di posta elettronica certificata nell'intento di evidenziare come tutti gli step dalla creazione di una e-mail fino alla messa a disposizione nella casella del destinatario siano accuratamente tracciati e documentati.
Schema di funzionamento[64]:



(63) Rif: CNIPA (*http://archivio.cnipa.gov.it/)*

(64) Immagine da: V.GAMBETTA, pag. 26 in *[27]*

In ogni dominio p.e.c. si possono individuare tre funzionalità:

- punto di accesso: consente l'accesso al servizio, effettua i controlli previsti per i messaggi da spedire e si occupa di generare la ricevuta di accettazione e la busta di trasporto;
- punto di ricezione: riceve i messaggi, effettua i dovuti controlli, genera la ricevuta di presa in carico e, se del caso, l'eventuale busta di anomalia;
- punto di consegna: provvede alla consegna del messaggio p.e.c. nella casella di posta elettronica del destinatario, dopo averne verificato la correttezza e la provenienza, ed emette la ricevuta di avvenuta consegna.

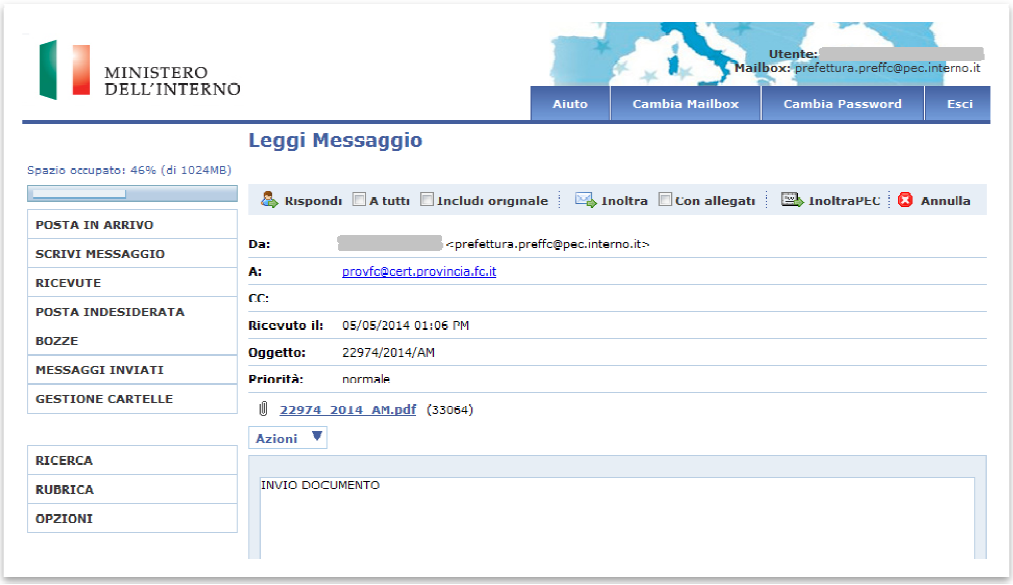
Il sistema di p.e.c. genera tre tipologie di messaggi costituiti da una parte di testo descrittivo per l'utente, e da una serie di allegati variabili a seconda della tipologia di messaggio:

- ricevute (di accettazione, di presa in carico, di avvenuta consegna);
- avvisi (di non accettazione, di mancata consegna);
- buste (di trasporto o di anomalia).

Le operazioni che si svolgono sono le seguenti:

1. Il mittente accede alla propria casella, compone il messaggio e lo invia(65).

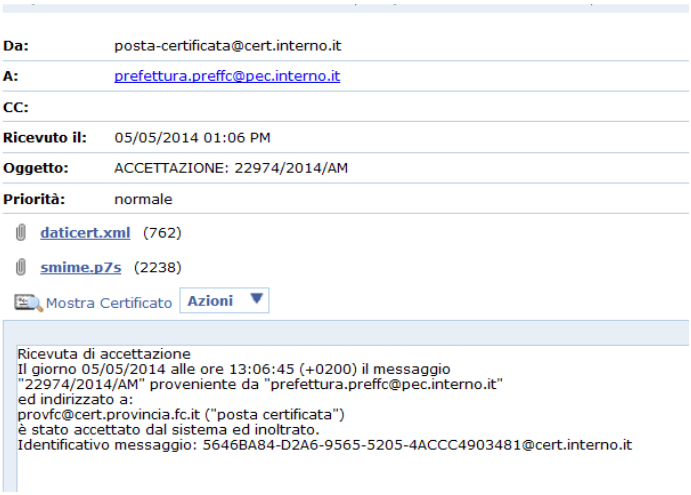
(65) Visualizzazione di una mail inviata da una casella p.e.c. ad un'altra casella p.e.c.:



2. Il gestore del mittente controlla le caratteristiche formali del messaggio, crea una *ricevuta di accettazione*[(66)], sottoscritta con firma elettronica, che contiene i dati di certificazione[(67)] e la invia al mittente. Nel caso il gestore rilevasse irregolarità formali, o presenza di virus informatici, invierà al mittente rispettivamente un avviso di non accettazione (con le relative motivazioni) o un avviso di non accettazione per virus informatico. In quest'ultimo caso, non solo è tenuto a non inoltrare l'e-mail, ma deve conservarla almeno per trenta mesi.

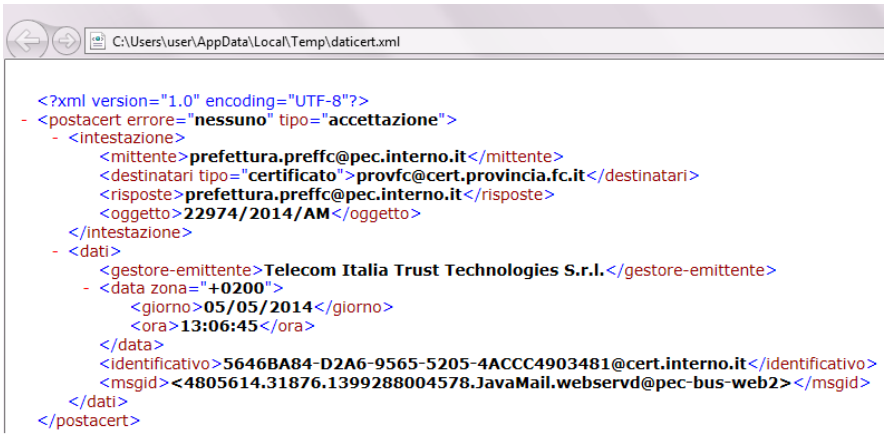
---

(66) Ricevuta di accettazione dell'e-mail p.e.c. inviata in (65) :



Il file *smime.p7s* contiene 2 certificati di cui è possibile verificare la validità e i dettagli tecnici:

Il file *daticert.xml* contiene i *dati di certificazione* che descrivono ed identificano il messaggio e sono generati e certificati dal gestore. Questi dati sono inseriti in un file XML (eXtensible Markup Language) che accompagna sempre, non solo le ricevute, ma anche le buste e gli avvisi.
Sotto è riportato il contenuto del file *daticert.xml*:



(67) I *dati di certificazione*, come dispone il DM 2 novembre 2005 sono i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.

3. Il messaggio viene "imbustato" in un altro messaggio, chiamato "*busta di trasporto*", che il gestore provvede a firmare, al cui interno sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione e lo invia al gestore del destinatario.

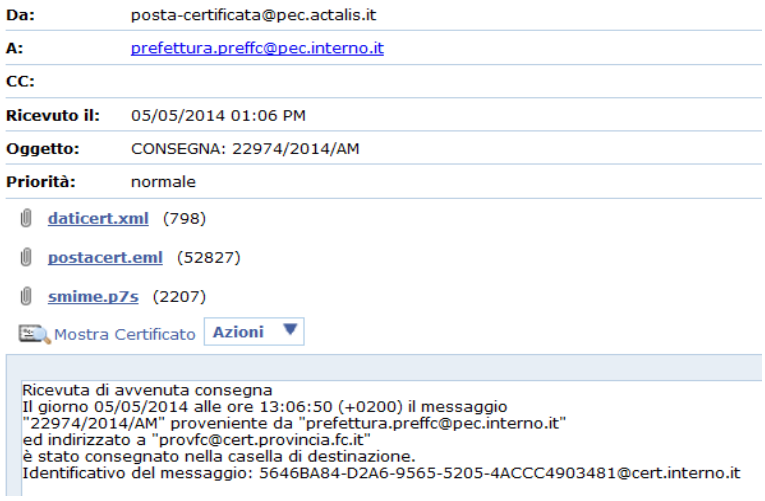
4. Il gestore del destinatario riceve la *"busta"* e controlla la validità della firma del gestore del mittente e la validità del messaggio, se tutti i controlli hanno avuto esito positivo, invia una *ricevuta di presa in carico* al gestore del mittente (trasparente al titolare ma allo scopo di consentire il tracciamento del messaggio nel passaggio tra un gestore ed un altro) e contemporaneamente rende disponibile il messaggio nella casella del destinatario. Se uno dei test, che il gestore del destinatario deve eseguire, evidenzia un errore nel messaggio in arrivo, oppure quest'ultimo è un messaggio di posta elettronica ordinaria e il gestore ne abbia previsto comunque l'inoltro al destinatario, il messaggio è inserito in una *"busta di anomalia"*, sottoscritta con la firma del gestore stesso, in tal caso nella busta è inserito un messaggio che evidenzia l'errore riscontrato ovvero che il messaggio trasportato non è certificato (in quanto il gestore ha l'obbligo di segnalare al titolare se l'e-mail non arriva da una casella p.e.c.).

5. Il destinatario riceve dal proprio gestore il messaggio nella propria casella di posta.

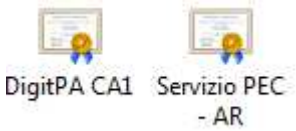
6. Il gestore del destinatario invia una *ricevuta di avvenuta consegna* alla casella del mittente[(68)].

---

(68) Ricevuta di consegna trasmessa al mittente dal gestore del destinatario:



Il file *smime.p7s* contiene 2 certificati di cui è possibile verificare la validità e i dettagli tecnici:



(Segue in [68bis])

7. La ricevuta di avvenuta consegna è emessa, nel formato richiesto dal mittente, infatti può essere richiesta una ricevuta completa, breve o sintetica. Se è richiesta la ricevuta completa, il gestore la invia con allegato il messaggio originale. Nella ricevuta breve è sempre associato il messaggio originale, ma gli eventuali allegati sono sostituiti con le loro impronte allo scopo di ridurre le dimensioni della ricevuta stessa. La ricevuta sintetica invece, contiene solo i dati di certificazione.
8. Il processo si conclude anche se il destinatario non ha ancora letto il messaggio.

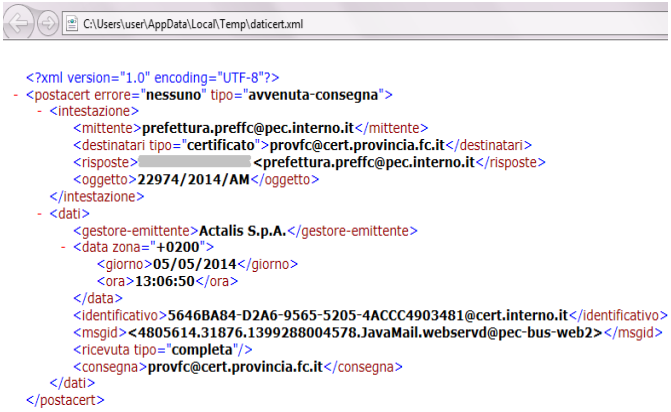
Nel caso in cui il gestore del mittente, entro le dodici ore successive all'inoltro del messaggio, non abbia ricevuto dal gestore del destinatario la ricevuta di presa in carico, o di avvenuta consegna del messaggio inviato, comunica al mittente l'eventualità che il messaggio possa non essere consegnato. Se, entro le successive dodici ore, al gestore del mittente non sia pervenuta la ricevuta di avvenuta consegna del messaggio inviato, questi inoltra al mittente un ulteriore avviso, relativo alla mancata consegna del messaggio, non prima di ventidue e non oltre ventiquattro ore successive all'invio.

I gestori di p.e.c. sono altresì tenuti alla conservazione del log dei messaggi, cioè del registro informatico delle operazioni relative alle trasmissioni effettuate, per ogni singola casella che gestiscono, per trenta mesi e sono tenuti ad adottare opportune soluzioni tecniche e organizzative tali da garantire riservatezza, sicurezza, integrità e

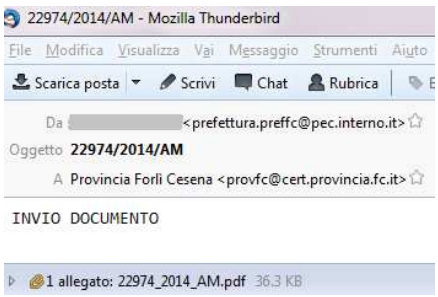
---

(68bis) La ricevuta di consegna contiene 3 allegati: i dati di certificazione, i certificati digitali e la mail originale in quanto all'invio il mittente ha, in questo caso, chiesto la ricevuta completa.

Il contenuto di *daticert.xml*:



Il contenuto della mail originale (*postacert.eml*):

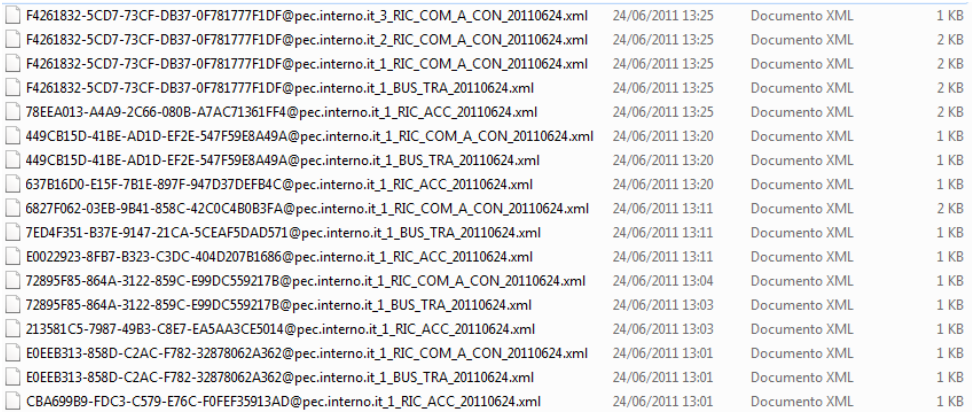


inalterabilità nel tempo di tali informazioni[(69)].

Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, egli può richiedere il log al gestore e tali informazioni sono opponibili ai terzi.

---

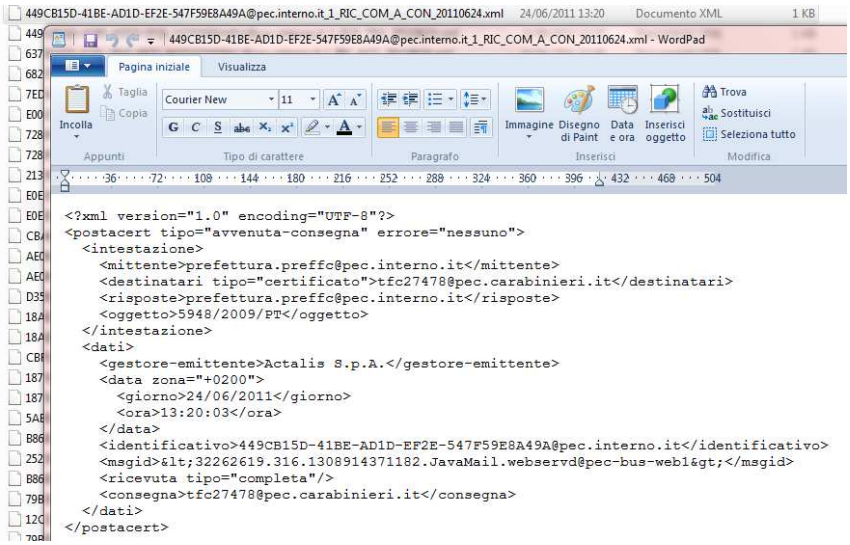
(69) Uno stralcio del log dei messaggi di una casella p.e.c. che il gestore deve essere in grado di produrre su richiesta del titolare:



Ognuno di questi file contiene i dati di certificazione dei singoli messaggi:

- il codice identificativo univoco assegnato al messaggio originale
- la data e l'ora dell'evento
- il mittente del messaggio originale
- i destinatari del messaggio originale
- l'oggetto del messaggio originale
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
- il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.)
- il gestore mittente

Il contenuto di uno di questi file:



Dall'analisi sin qui compiuta del servizio di posta elettronica certificata, tutte le "debolezze" della posta elettronica ordinaria, riferite all'inizio di questo capitolo, si mostrano ampiamente superate. La ricevuta di accettazione costituisce a tutti gli effetti prova dell'avvenuta spedizione e la ricevuta dell'avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna[(70)] tramite un testo, leggibile dal mittente, contenente i dati di certificazione.

In merito alle trasmissioni ad una pubblica amministrazione, l'invio fatto da una casella di posta elettronica certificata, che costituisce uno strumento idoneo ad accertare la provenienza della comunicazione, soddisfa il requisito della forma scritta e la trasmissione non deve essere seguita dal documento originale. Salvo che la legge non disponga diversamente, questo tipo di trasmissione equivale alla notificazione per mezzo della posta tradizionale secondo il disposto degli artt. 45 e 48 del Codice dell'Amministrazione Digitale.

Con riferimento alla valenza giuridica delle ricevute di trasmissione via posta elettronica certificata, si cita la sentenza n. 2677/2013 del TAR della Lombardia dove è stata approfonditamente esaminata l'ipotesi in cui una stazione appaltante abbia provveduto a comunicare ai partecipanti l'intervenuta aggiudicazione definitiva attraverso l'invio di un messaggio di posta elettronica certificata, con particolare riferimento alla decorrenza del termine di 30 giorni utili dall'avvenuta comunicazione, per presentare ricorso. Nella sentenza viene espressa la tesi, secondo cui, la posta elettronica certificata integra *ex lege* uno strumento di comunicazione di per sé idoneo a determinare la conoscenza rilevante per la decorrenza del termine di impugnazione. Nel caso specifico, si è proceduto all'analisi della ricostruzione normativa e all'individuazione di quale sia in concreto il momento a decorrere dal quale si producono gli effetti connessi alla comunicazione via p.e.c.. E' stato ritenuto che la comunicazione dell'aggiudicazione, effettuata a mezzo di posta elettronica certificata, si intende avvenuta nella data indicata nella ricevuta di avvenuta consegna fornita al mittente dal

(70) A ciascuna trasmissione è apposto un unico riferimento temporale generato con un sistema tale da garantire stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di Tempo Universale Coordinato (UTC).

gestore di posta elettronica certificata utilizzato dal destinatario e, poiché la ricevuta di avvenuta consegna è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario, il momento in cui il destinatario legge il messaggio è del tutto irrilevante ai fini della conoscenza legale del documento trasmesso(71).

E' importante evidenziare, in chiusura del presente capitolo, che sussiste una differenza sostanziale che intercorre tra la ricezione di un documento via p.e.c. e la ricezione via raccomandata: nel primo caso si considera sempre ricevuto una volta consegnato nella casella di posta dal gestore del sistema del destinatario (artt. 45 e 48 C.A.D.), nell'altro la consegna richiede la presenza fisica del destinatario o di un suo delegato che hanno firmato per riceverlo. Stante quanto detto, sia per la ricevuta di consegna di una e-mail p.e.c. che per la ricevuta di ritorno di una raccomandata ordinaria si fa ricorso alla presunzione di conoscenza(72) di cui all'art. 1335 c.c. che così dispone: *"La proposta, l'accettazione, la loro revoca e ogni altra dichiarazione diretta a una determinata persona si reputano conosciute nel momento in cui giungono all'indirizzo del destinatario, se questi non prova di essere stato, senza sua colpa, nell'impossibilità di averne notizia"*.

---

(71) Sentenza TAR Lombardia, Milano, n. 2677/2013 del 3.12.2013. Rif: R.BIANCHINI in *[29]*

(72) Per *presunzione* (o *prova indiretta*) si intende ogni argomento, congettura, illazione, avverso cui, essendo già provata una determinata circostanza (cd. *fatto base* o *indizio* si giunge a considerare provata altresì un'altra circostanza, sfornita di prova diretta (ad es., dalla circostanza che sia decorso già un certo periodo di tempo dal momento in cui si poteva pretendere il pagamento di determinati debiti, per i quali è regola di esperienza che il pagamento avviene entro breve tempo, si trae la presunzione che il debito sia già stato pagato o comunque si sia già estinto, sebbene manchino prove dirette del pagamento o del verificarsi di un'altra causa di estinzione dell'obbligo).
Le presunzioni sono *legali* quando è la legge stessa che, in via generale, attribuisce ad un fatto il valore di prova in ordine ad un altro fatto, che viene quindi presunto, ad esempio che chi ha il possesso di una cosa altrui sia in buona fede (art. 1147 comma 3 c.c.). oppure la presunzione che una dichiarazione diretta ad una determinata persona sia da quest'ultima conosciuta nel momento in cui la stessa giunge al suo indirizzo (art. 1335 c.c.). Le presunzioni legali possono essere *iuris de iure* se non ammettono prova contraria o *iuris tantum* se la ammettono, in tali casi la prova contraria può essere fornita facendo ricorso a qualunque mezzo. Ci sono però casi in cui la legge pone limitazioni ai mezzi di prova utilizzabili o all'oggetto della prova contraria, come all'art. 1335c.c.. Le presunzioni si dicono invece *semplici* (*o hominis*) , quando non sono prestabilite dalla legge e sono lasciate al prudente apprezzamento del giudice.
Rif: A.TORRENTE – P.SCHLESINGER, pagg. 251-252 in *[2]*

3. Come ottenere il domicilio digitale

"La dematerializzazione dei rapporti con la pubblica amministrazione, il cosiddetto switch off, ovvero l'abolizione di ogni interazione fisica e cartacea, è uno strumento potentissimo per semplificare la vita delle imprese e dei cittadini, riducendo il costo e il peso della burocrazia, facendo risparmiare tempo e denaro, migliorando la qualità di tutti i servizi erogati. Semplificare digitalizzando, questo è il principio ispiratore che accomuna tali provvedimenti. Disporre di una identità e di un domicilio digitale, raggruppare e rendere interoperabili le anagrafi per avere una visione a tutto tondo, rappresenta un passo estremamente significativo per rendere più immediati, veloci e trasparenti i rapporti fra cittadino e pubblica amministrazione" [(73)].

Quanto appena riportato è contenuto nella relazione illustrativa al D.L. 179/2012, recante ulteriori misure urgenti per la crescita del paese, il c.d. *Decreto Crescita 2.0* (altresì detto *Decreto Sviluppo Bis)*, che ha introdotto nel Codice dell'Amministrazione Digitale il diritto del cittadino all'assegnazione del domicilio digitale. L'attribuzione da parte dello Stato di un indirizzo di posta elettronica certificata gratuita e volontaria era già stato introdotto dal legislatore con il D.L. 185/2008, il c.d. *Decreto Anticrisi*, convertito con modificazioni dalla Legge 2/2009.

In questo capitolo si discuterà innanzitutto della Postacertificat@ o CEC-PAC, il servizio introdotto in ottemperanza alla legge appena citata, delle sue funzionalità e della risposta dei cittadini a questo servizio. Si tratterà poi, nello specifico, del domicilio digitale come introdotto dal *Decreto Sviluppo Bis* e come da ultimo, con riferimento al D.L. 69/2013, c.d. *Decreto del Fare*, convertito con modificazioni dalla Legge n. 98/2013, si sia parlato di *"resurrezione della CEC-PAC"*[(74)], cioè di un indirizzo di posta elettronica certificata, assegnato *d'ufficio* che costituirà (ad oggi manca un decreto attuativo specifico) il domicilio digitale e troverà posto, come ulteriore dato personale, nell'Anagrafe Nazionale della Popolazione Residente.

---

(73) Cit: Relazione al Disegno di Legge di conversione del Decreto Legge 2012, n.179, recante ulteriori misure urgenti per la crescita del Paese, Diritto24 - Il sole24ore, pag. 2 *(http://www.diritto24.ilsole24ore.com/civile/civile/news/2012/10/decreto-legge-18-ottobre-2012-n-179-recante-ulteriori-misure-urgenti-per-la-crescita-del-paese-dl-sviluppo-bis---testo-integrale.php)*

(74) Cit: L.FOGLIA in *[37]*

3.1 La Postacertificat@ per il cittadino

Con la Legge di conversione n. 2/2009 viene introdotto, nel D.L. 185/2008, l'art. 16-bis contenente "*Misure di semplificazione per le famiglie e per le imprese*".

Tra le diverse disposizioni per agevolare il cittadino nei rapporti con la pubblica amministrazione, il comma 5 dispone che, per favorire la realizzazione degli obbiettivi di massima diffusione delle tecnologie telematiche nelle comunicazioni, previste dal C.A.D., ai cittadini che ne fanno richiesta, è attribuita gratuitamente una casella di posta elettronica certificata, o analogo indirizzo 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. Senza dubbio si può certamente affermare che "*ancora una volta, alla pubblica amministrazione è affidato il ruolo di volano nella informatizzazione della comunicazione e dei servizi, come già è accaduto, ad esempio, per la firma digitale*"[(75)].

Le modalità di richiesta, attivazione ed utilizzo di tale casella di posta elettronica certificata, delle quali si tratterà di seguito, sono definite dal D.P.C.M. 6 maggio 2009.

I cittadini che ne fanno richiesta, alla Presidenza del Consiglio dei Ministri - Dipartimento per la digitalizzazione della Pubblica Amministrazione e per l'innovazione tecnologica (DDI), hanno diritto all'assegnazione di un indirizzo p.e.c., rilasciato ai sensi degli artt. 6 e 48 del C.A.D., che consente la trasmissione e la ricezione telematica di documenti che necessitano di una ricevuta di invio e di una di consegna e la cui trasmissione equivale, salvo che la legge non disponga diversamente, alla notificazione per mezzo della posta.

La casella certificata, ottenuta attraverso il servizio di Postacertificat@, diviene sostanzialmente domicilio informatico[(76)], in quanto l'attribuzione, seppure su richiesta volontaria perfezionata al momento dell'attivazione, comporta l'accettazione *tout court* dell'invio, su quella specifica casella, di tutti i provvedimenti che riguardano il cittadino da parte delle pubbliche amministrazioni.

---

(75) Cit: G.FINOCCHIARO in *[30]*

(76) Rif: G.FINOCCHIARO in *[30]*

Va ricordato che, nel momento in cui sussiste la ricevuta di consegna, si presume secondo i principi generali, ed in particolare secondo l'art. 1335 c.c.[77], la conoscenza del contenuto della trasmissione; ed è quindi a carico del cittadino, la prova dell'essere stato, senza sua colpa, nell'impossibilità di averne notizia[78].

La gestione del servizio di casella p.e.c. gratuita, identificata con la sigla CEC-PAC ("*Servizio di Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino"*) è stata affidata in concessione al raggruppamento temporaneo di imprese costituito da Poste Italiane S.p.A, Postecom S.p.A. e Telecom Italia S.p.A. ed è attiva dal 26 aprile 2010.

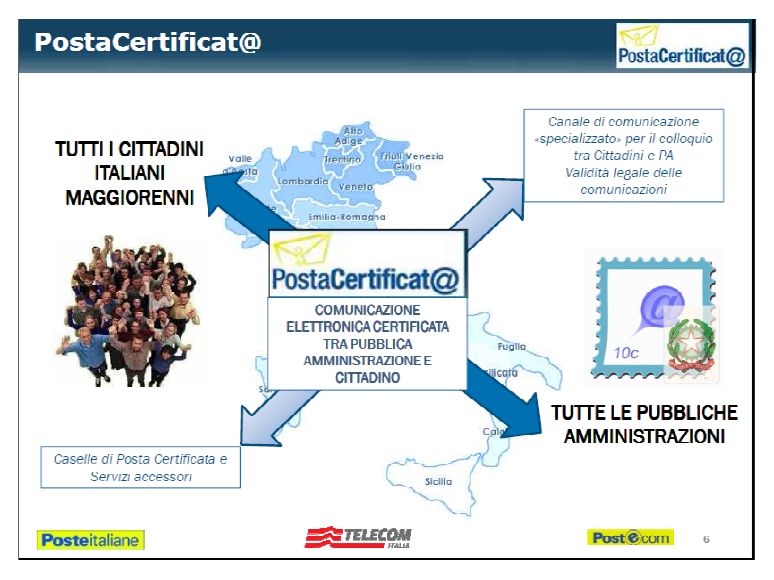
Il servizio è stato accompagnato da un'ampia campagna informativa mirata a stimolarne la richiesta di attivazione. La pubblicità di tale iniziativa è stata disposta anche dall'art. 8 del D.P.C.M. stesso: *"La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie cura la realizzazione di campagne di comunicazione volte a diffondere e pubblicizzare i contenuti dell'iniziativa e le modalità di rilascio e di uso della casella di PEC ai cittadini, con particolare riguardo alle categorie a rischio di esclusione ai sensi dell'art. 8 del decreto legislativo n. 82 del 2005"*.

---

[77] Art 1335 c.c.: "*Presunzione di conoscenza - la proposta, l'accettazione, la loro revoca e ogni altra dichiarazione diretta a una determinata persona si reputano conosciute nel momento in cui giungono all'indirizzo del destinatario, se questi non prova di essere stato, senza sua colpa, nell'impossibilità di averne notizia"*.

[78] Come per altro ben specificato nella guida all'utente del servizio: "*Si ricorda che la casella PostaCertificat@ del cittadino, una volta rilasciata, è l'unico indirizzo valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni e richiedendo la casella si elegge la casella PostaCertificat@ ad unico indirizzo per la comunicazione con la Pubblica Amministrazione. In caso di smarrimento, furto o perdita della stessa, si raccomanda di seguire immediatamente le procedure per il reset/cambio della password. In caso di evidente o sospetto uso improprio della casella da parte di terzi a seguito di furto o forzatura della password, si raccomanda di denunciare immediatamente l'accaduto alle autorità competenti" (https://www.postacertificata.gov.it /guida_utente/servizi/servizi.dot)*

Nelle due immagini[79], qui a seguire riportate, sono ben evidenziati gli obbiettivi da raggiungere: ridurre le distanze tra il cittadino e la pubblica amministrazione attraverso l'utilizzo di una casella certificata, non solo per ottenere celermente certificati e altri documenti burocratici per via telematica, ma anche come strumento di riconoscimento ed accesso ai servizi.



(79) Rif. immagini: G.ZAPPA n. 6 e n. 8 in *[32]*

Obbiettivi ben evidenziati anche dalla Presidenza del Consiglio dei Ministri durante la conferenza stampa di presentazione del 26 aprile 2010[80]:

L'attivazione della casella è consentita a tutti i cittadini italiani maggiorenni (anche se residenti all'estero) e a tutti i cittadini maggiorenni di nazionalità straniera residenti nel territorio italiano in possesso di un codice fiscale e, se cittadini extra-UE, di permesso di soggiorno (permesso di soggiorno CE per soggiornanti di lungo periodo, ex art. 9 del T.U. Immigrazione di cui al D.Lgs. 286/1998) o "modello 22A con Ologramma" (rilasciato dagli Uffici Postali all'atto della presentazione del kit per il rinnovo del permesso di soggiorno).

[80] Rif. immagini: PRESIDENZA CONSIGLIO MINISTRI, pag. 4 e pag. 10 in *[33]*

Tutte le pubbliche amministrazioni centrali e locali possono richiedere l'attivazione di caselle PostaCertificat@ anche per i propri dipendenti.

Sul sito internet[81] vengono ben dettagliati i *servizi di base* che vengono forniti gratuitamente all'attivazione e i servizi avanzati che invece hanno un costo e devono essere attivati singolarmente.

I *servizi di base* forniti in forma gratuita sono:

- Casella di posta elettronica PostaCertificat@;
- Servizio opzionale di notifica tramite posta elettronica tradizionale (ad esempio dell'avvenuta ricezione di un messaggio sulla propria casella PostaCertificat@, oppure delle ricevute di accettazione e consegna conseguenti ad un invio);
- Fascicolo elettronico personale, cioè uno spazio per la memorizzazione dei documenti scambiati, pari a 1 GB;
- Indirizzario delle pubbliche amministrazioni provviste di PostaCertificat@ o di posta elettronica certificata, i cui dati vengono attinti dall'Indice delle P.A..

I *servizi avanzati* a pagamento:

- Firma digitale;
- Calendario degli eventi, con l'indicazione delle principali scadenze d'interesse;
- Servizi di notifica con SMS, ossia di segnalazione, attraverso SMS, degli eventi collegati alla casella stessa o al Calendario degli eventi.

(81) Immagine del portale di accesso ai servizi di Postacertificat@: *https://www.postacertificata.gov.it/*

E’ inoltre prevista, al momento in cui si scrive, l’attivazione di ulteriori *servizi avanzati* a pagamento:

- Firma Digitale Remota;
- Posta On Line;
- Pagamento Ticket Sanitari;
- Rilascio Certificati Anagrafici.

Per attivare la casella occorre registrarsi sul portale web con i propri dati anagrafici, scegliere i servizi di interesse, esprimere esplicita accettazione delle condizioni contrattuali per avviare la richiesta e scegliere una PASSWORD con cui si accederà alla casella. La USER-ID assegnata sarà *nome.cognome* e la casella sarà *nome.cognome@postacertificata.gov.it* (le omonimie verranno gestite attraverso l’uso di codici numerici).

Una volta effettuata la registrazione è necessario attuare la procedura di attivazione, che consiste nel recarsi personalmente (a partire dalle 24 ore successive e comunque entro 3 mesi dalla registrazione) presso uno degli uffici postali abilitati al servizio per le attività di identificazione e firma del contratto e dell'informativa sulla privacy. L’utenza, all'interno del sistema di gestione delle identità del Portale PostaCertificat@, sarà attivata entro le 24 ore successive ed il cittadino potrà accedere alla propria casella ed eseguire le attività connesse al proprio profilo.

Se si è effettuata la richiesta di attivazione del servizio PostaCertificat@, ma non si vuole completarla recandosi ad un Ufficio Postale per l’identificazione, si può procedere all’annullamento direttamente sul sito.

In qualunque momento si potranno modificare i propri dati personali e anche recedere dal servizio, sempre attraverso il sito. Il recesso comporta, oltre alla cessazione dal servizio, la cancellazione dagli elenchi contenenti gli indirizzi di posta elettronica certificata dei cittadini entro ventiquattro ore dall'avvenuta comunicazione del recesso. In conseguenza del recesso, le comunicazioni tra il cittadino e la p.a. si realizzano secondo le procedure tradizionali.

Dal punto di vista più strettamente funzionale:

- la casella CEC-PAC ha dimensione di 250 MB;
- il numero massimo di invii giornalieri non può essere superiore a 10;
- la dimensione massima del messaggio non può superare i 30 MB;

- il numero massimo di destinatari di una e-mail non può essere superiore a 50;
- il tempo che si ha a disposizione per scrivere il messaggio che è di dieci minuti;
- è consultabile tramite un browser attraverso il portale web su apposita area riservata e/o attraverso un client di posta elettronica;
- garantisce canali sicuri in quanto le comunicazioni sono realizzate utilizzando protocolli di trasmissione dati crittografati (si utilizzano Transport Layer Security – TLS e Secure Sockets Layer – SSL);
- il sistema include componenti antivirus che effettuano controlli sia nei messaggi in ingresso che in uscita;
- tutti i log dei messaggi scambiati sono memorizzati su un registro riportante i dati significativi dell'operazione e sono conservati per 30 mesi dall'affidatario del servizio;
- si potrà altresì richiedere copia delle notifiche dei messaggi di PostaCertificat@ relativi ad un determinato periodo.

Il servizio di Postacertificat@, come evidenziato nella conferenza stampa di presentazione[(82)], avvicina all'idea dell'associazione tra la posta certificata per il cittadino e la carta di identità elettronica. Vero è che viene consentito l'accesso anche attraverso l'autenticazione effettuata tramite smart-card, emesse dalle amministrazioni preposte (quali la Carta Nazionale dei Servizi e la Carta di Identità Elettronica), in alternativa a user-id e password.

(82) Rif. immagine: PRESIDENZA CONSIGLIO MINISTRI, pag. 9 in *[33]*

Questa funzionalità è resa possibile ai soli utenti (registrati o preregistrati) che dispongono già di una smart-card con certificato valido e il codice PIN che consente l'identificazione on-line del titolare[(83)].

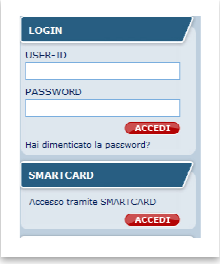
Gli indirizzi p.e.c. dei cittadini saranno resi consultabili, in via telematica alle pubbliche amministrazioni dall'affidatario del servizio, nel rispetto dei criteri di qualità, sicurezza ed interoperabilità definiti dal CNIPA e nel rispetto della disciplina in materia di tutela dei dati personali di cui al D.Lgs. 30 giugno 2003, n. 196. Dal canto loro, le pubbliche amministrazioni di cui all'art. 1, comma 2 del D.Lgs. 165/2001[(84)], che sono tenute ad istituire una casella p.e.c. per ogni registro di protocollo e a darne comunicazione al CNIPA per la pubblicazione su IndicePa, devono accettare le istanze dei cittadini inviate tramite p.e.c. nel rispetto dell'art. 65, comma 1, lettera c-bis) del C.A.D. stante che l'invio tramite p.e.c. costituisce firma elettronica ai sensi dell'art. 21, comma 1, del Codice stesso.

3.2 La Postacertificat@ e le altre

In considerazione delle caratteristiche funzionali della Postacertificat@ per il cittadino prevista dall'art. 16-bis comma 5 del D.L. 185/2008, si affronterà il tema delle comunicazioni tra le diverse tipologie di caselle di posta elettronica certificata esistenti.

---

(83) L'immagine sottostante, estratta dal portale *https://www.postacertificata.gov.it/* mostra le due possibili modalità di accesso. E' consentito l'utilizzo di tutte le Smart Card, CNS/CIE, emesse dalle pubbliche amministrazioni preposte. La CNS/CIE è un documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta. Utilizza una carta a microprocessore in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. Per richiedere la CNS/CIE il cittadino deve rivolgersi direttamente agli uffici competenti preposti della Pubblica Amministrazione.
(Rif: *https://www.postacertificata.gov.it/guida_utente/guida-utente.dot*)



(84) Si riporta quanto previsto dall'art. 1, comma 2 del Decreto Legislativo 30 marzo 2001, n. 165:
"Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale".

La casella di Postacertificat@, per il cittadino che ne ha chiesto il rilascio, va a costituire l'unico indirizzo valido ad ogni effetto giuridico ai fini dei rapporti con le pubbliche amministrazioni.

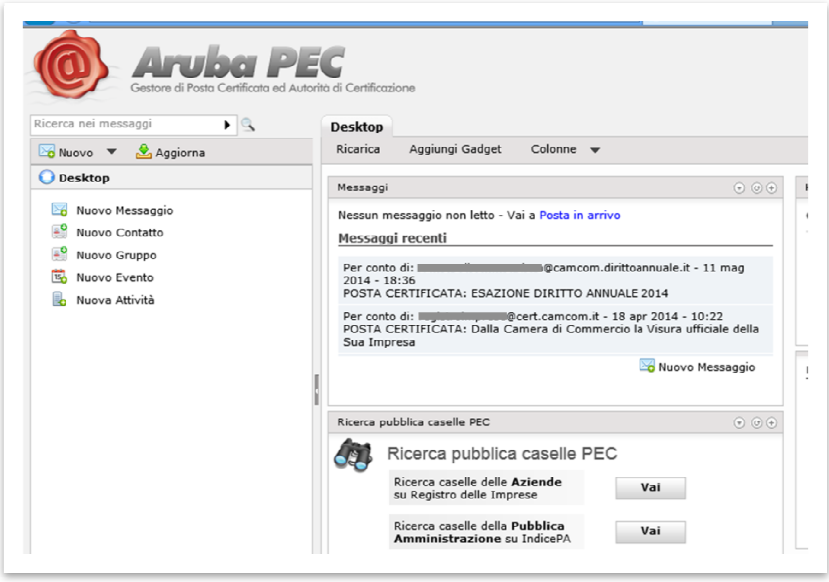
D'altra parte l'art. 16 del medesimo decreto legge ha disposto, per le imprese costituite in forma societaria e per i professionisti iscritti ad albi, l'obbligatorietà di una casella p.e.c. alla quale potranno essere inviate comunicazioni, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo; l'obbligo di titolarità di una casella p.e.c. sarà poi introdotto dal D.L. 179/2012 anche alle imprese individuali.

Una prima differenza da rilevarsi è che le caselle di Postacertificat@ per il privato cittadino sono attribuite gratuitamente dallo Stato, diversamente dalle p.e.c. per le imprese e i professionisti, che devono necessariamente essere acquistate sul mercato privato offerto dai gestori autorizzati dall'Agenzia per l'Italia Digitale.

La diversità sostanziale però, tra queste due tipologie di comunicazione elettronica certificata, al di là del fattore economico, è ben più ampia: le caselle di posta elettronica certificata acquistate dall'offerta privata dei gestori, possono comunicare con qualsiasi altro indirizzo p.e.c.[(85)], in virtù dell'obbligo di interoperabilità e del rispetto

---

(85) Interfaccia tipica per l'utente di una casella p.e.c. rilasciata da un gestore privato che consente di inviare e-mail a qualunque indirizzo p.e.c. o di posta elettronica ordinaria. Queste caselle mettono a disposizione ricerca delle aziende sull'INI-PEC e delle p.a. su IndicePA:



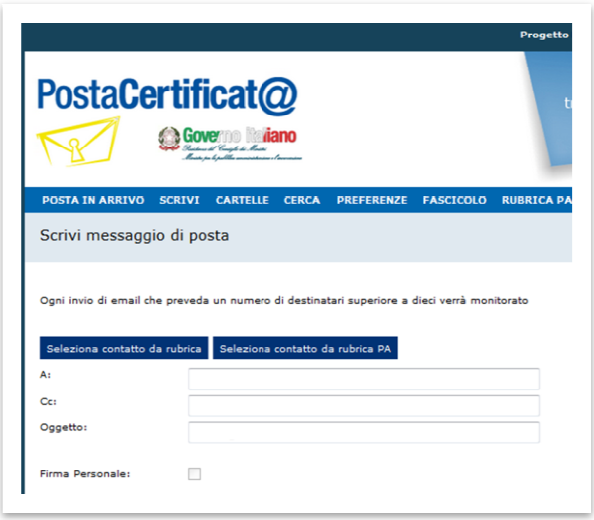
degli standard fissati per legge, e al contempo possono comunicare anche con gli indirizzi di posta elettronica ordinaria[86].

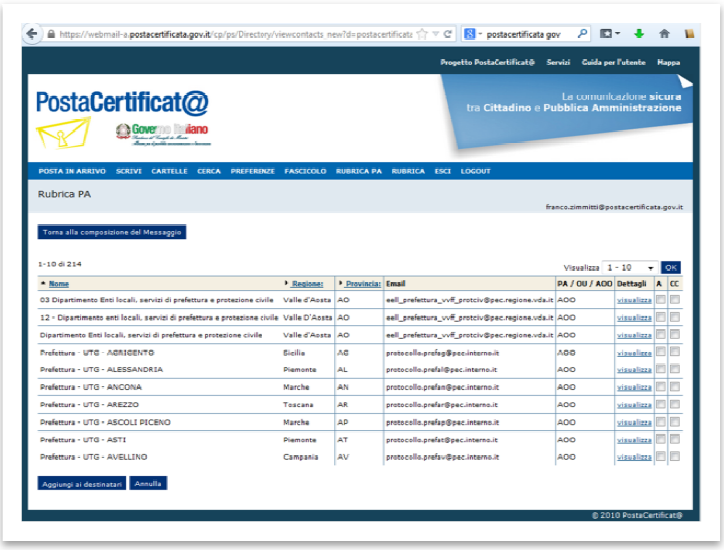
Il cittadino titolare di casella Postacertificat@ può inviare o ricevere solo da caselle presenti in IndicePA[87]: non è in alcun modo consentito l'invio di e-mail da Postacertificat@ ad una casella di posta elettronica ordinaria o ad una casella di Postacertificat@ di un altro cittadino o ad una p.e.c..

---

[86] L'invio di una e-mail da una casella p.e.c. ad una casella di posta elettronica ordinaria avviene regolarmente anche se il mittente disporrà solo della ricevuta di accettazione fornita dal proprio gestore p.e.c. In pari misura è possibile inviare da una casella di posta elettronica ordinaria un'e-mail ad una casella p.e.c., tuttavia il titolare della casella p.e.c. destinataria potrebbe rifiutare l'e-mail non essendo certificata.

[87] Nelle due immagini sottostanti è riportata l'interfaccia di Postacertificat@ di produzione di una e-mail e la rubrica in linea degli indirizzi di posta elettronica certificata delle pubbliche amministrazioni iscritte in IndicePA:

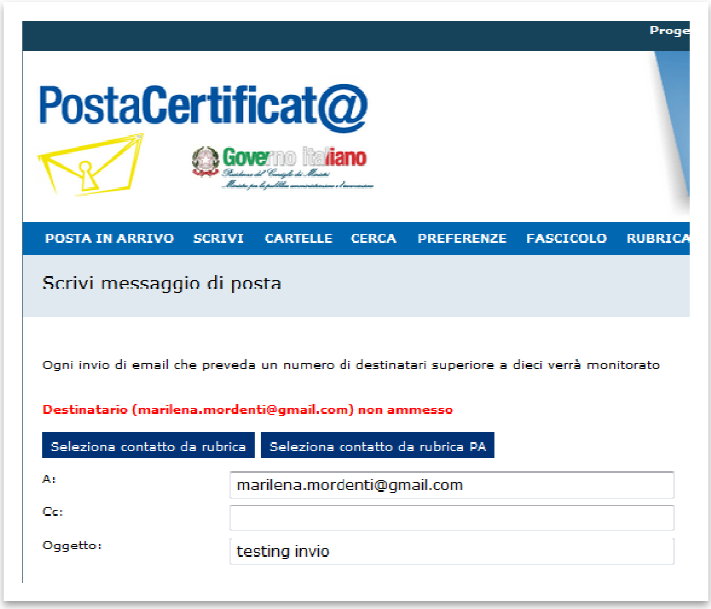


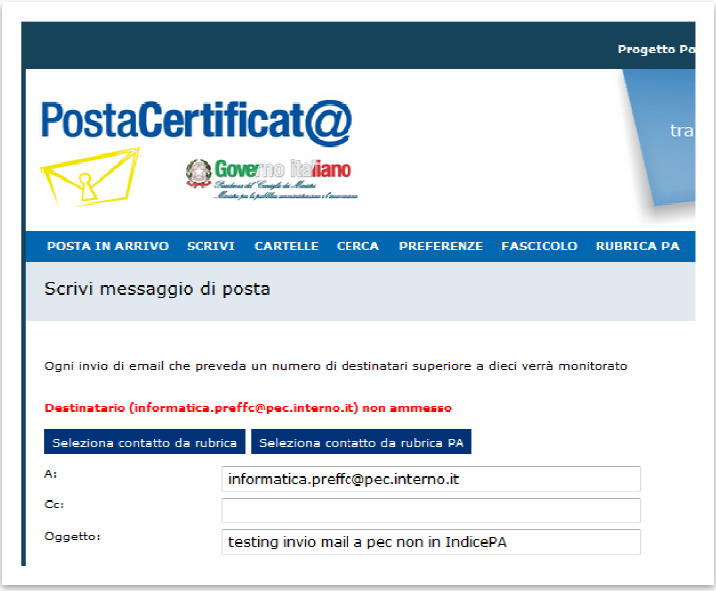


Sono consentite solo le comunicazioni con le caselle di posta elettronica certificata delle pubbliche amministrazioni presenti in IndicePa[88].

Si tratta sostanzialmente di mondi separati, o per meglio spiegare, si può dire che la CEC-PAC è sostanzialmente un sottoinsieme di posta elettronica certificata con servizi più limitati[89].

[88] Si riportano, a titolo di esempio, le risposte ricevute dal servizio di Postacertificat@ al tentativo di inviare una e-mail ad una casella di posta ordinaria e ad una casella p.e.c., seppure quest'ultima di una pubblica amministrazione ma non presente in IndicePA:





[89] Rif: G.P.DORIA in *[31]*

Tale scelta potrebbe, presumibilmente, essere ricondotta a due motivazioni fondamentali: la prima è che questo servizio è nato con l'intento dichiarato di migliorare e semplificare i rapporti tra il cittadino e la pubblica amministrazione riducendo i tempi di risposta per gli utenti e le spese postali a carico dello Stato, la seconda si può presumere sia quella di non turbare il mercato dei servizi p.e.c. già gestiti, al tempo dell'istituzione della CEC-PAC, dal settore privato(90)(91). Va aggiunto, inoltre, che la casella di Postacertificat@ non può considerarsi utile ai fini dell'assolvimento degli obblighi di comunicazione previsti per la realizzazione dell'INI-PEC a partire dagli elenchi di indirizzi p.e.c. costituiti presso il Registro delle imprese e gli ordini o collegi professionali. L'obbligo in questione non può essere assolto mediante l'indicazione della CEC-PAC fornita dalle imprese e dai professionisti, ne consegue pertanto che il Registro delle Imprese e gli ordini e collegi professionali dovranno rifiutare tutti questi indirizzi di posta elettronica certificata, che siano costituiti in forma di CEC-PAC, contraddistinti dal dominio @postacertificata.gov.it(92).

(90) *"Perché si è scelto un servizio di posta "chiusa", soltanto per i rapporti fra PA-cittadini, e non di utilizzare il già previsto servizio di Pec? Il problema riguarda principalmente gli aspetti legati all'uso di standard di natura giuridica e di processi organizzativi che dipendono non solo dall'Italia, ma anche dalla Ue. Un servizio di posta certificata aperta, dato gratuitamente ai cittadini - con la funzione prevalente di elezione di domicilio digitale - anche se snatura in un certo senso il tradizionale servizio di Pec gestito dai privati, crea meno problemi di un servizio di Pec nazionale gratuito che, certamente, sarebbe un precedente che potrebbe dare fastidio a tutte le società private che gestiscono i servizi di posta. I colossi postali internazionali non vedono di buon occhio la diffusione di uno strumento a costo zero che andrebbe a erodere il business delle raccomandate".* Cit: A.MAZZEO in *[34]*

(91) Rif: G.ROGNETTA in *[35]*

(92) Si riporta il contenuto della circolare del Ministero dello Sviluppo economico del 15/1/2014 che conferma l'impossibilità di fornire un indirizzo di Postacertificat@ ai fini dell'iscrizione nell'Ini-Pec:
"Sono pervenuti allo scrivente Ministero numerosi quesiti da parte di Ordini e Collegi professionali relativamentte alla possibilità di utiilizzare, da parte dei professionisti iscritti nei medesimi, la cosiddetta CEC-PAC quale indirizzo di posta elettronica certificata, rilevante a norma dell'articolo 16, comma 6 del decreto legge n. 185 del 2008 e dell'articolo 6-bis, c. 2, d.lgs. n. 82/2005 (codice dell'amministrazione digitale –CAD). In proposito si rammenta che questa Amministrazione, con propria nota del 10 settembre 2013 rivolta alle Camere di commercio, si era già pronunziata in merito alla stessa fattispecie con riguardo alle imprese individuali, per le quali l'articolo 5 del decreto legge 179 del 2012 imponeva il medesimo obbligo di dotazione di un indirizzo di posta elettronica certificata. In quell'occasione si ebbe ad affermare che per gli uffici del registro delle imprese l'obbligo in questione, relativo alla comunicazione all'INI-PEC degli indirizzi PEC da loro detenuti delle imprese individuali, non potesse essere assolto mediante l'indicazione della CEC-PAC (posta elettronica certificata del cittadino), stante la differente funzione riconnessa a quest'ultimo indirizzo rispetto a quello da trasmettere all'INI-PEC, nonchè per le modalità particolari di rilascio della CEC-PAC stessa". (Segue in 92bis)

Le caselle di Postacertificat@, regolarmente attivate dall'aprile 2010 a febbraio 2014, sono circa 1,7 milioni[93]. Le aspettative, al momento in cui il servizio è stato reso operativo, erano ben più ottimistiche: in buona sostanza, decorsi già quattro anni dalla nascita, era lecito attendersi un numero maggiore di adesioni. Le motivazioni di questo scarso successo sono certamente molte e tutte correlate.

La prima cosa da dire è che, nel 2010 molte amministrazioni locali, ci si riferisce soprattutto a quelle più vicine ai cittadini, cioè i comuni, rendevano già disponibili molte informazioni e modulistica oltre a diversi servizi on-line (concordemente con quando il C.A.D. chiedeva) ed avevano quindi già consolidato l'utilizzo di specifiche forme di comunicazione digitale tramite il loro portale istituzionale.

La Postacertificat@, dal canto suo, non è mai stata di fatto resa obbligatoria e il cittadino non ne ha percepito la necessità, non essendo stata integrata in un piano organico di e-Government che potesse inviare un segnale di utilità reale. *"Un servizio che, di certo, funzionerebbe è quello della notifica delle cartelle delle tasse, ma non credo che la cosa entusiasmi tanto i destinatari, convincendoli a superare tutta la burocrazia legata all'acquisizione di una tale casella"*[94].

Probabilmente il cittadino è stato frenato dall'idea di essere obbligato alla consultazione della casella, dal momento in cui l'avesse attivata, in quanto la stessa ha anche valore di *"domicilio fiscale, e che rappresenta, quindi, un posto dove poter inviare multe, cartelle esattoriali. Agli italiani non piace non avere il controllo della propria corrispondenza, soprattutto quando si tocca il tasto dolente delle sanzioni. Con*

(92bis) *"Questa, infatti, pur costituendo una normale modalità di posta elettronica per il cittadino (peraltro rilasciata gratuitamente), permette tuttavia di comunicare esclusivamente con la Pubblica Amministra-zione e non può essere utilizzata per comunicazioni ufficiali tra aziende o tra cittadini. Stante quanto sopra, si rappresenta che le considerazioni sopra svolte debbono trovare pedissequa applicazione anche nel caso delle predette CEC-PAC dei professionisti, tenuto conto peraltro del concorde avviso espresso in proposito dall'AgID - Agenzia per l'Italia Digitale - con nota del 10 dicembre 2013, a seguito di esplicita richiesta di parere da parte dello scrivente. Ne consegue pertanto che ai fini della formazione ed aggiornamento INI-PEC verranno rifiutati tutti quegli indirizzi di posta elettronica certificata comunicati da codesti Ordini e Collegi che siano costituiti in forma di CEC-PAC (pec al cittadino), contraddistinti dal dominio @postacertificata.gov.it."*

(93) Rif: F.META in *[36]*

(94) Rif: A.MAZZEO in *[34]*

la Cec-Pac, infatti, una volta inviato il plico telematico e ricevuto il messaggio di ritorno, l'ente dà per notificato il documento a prescindere dall'apertura del messaggio di posta da parte del cittadino"[(95)].

Dall'altro lato le pubbliche amministrazioni spesso si sono ritrovate a dover usare strumenti nuovi che non sono riuscite ad integrare pienamente nei processi organizzativi interni. Questo richiede certamente tempo, in quanto, trattandosi di posta elettronica certificata, occorre inserirne l'utilizzo in un più ampio processo di trattamento documentale elettronico che investa tutti i processi amministrativi. Tutto ciò impatta negativamente nell'interazione con il cittadino al quale sono stati offerti pochi servizi non integrati tra loro. Senza poi parlare dei soggetti che *"soffrono di 'analfabetismo informatico'"* e quindi non hanno alcun interesse in quanto *"il servizio non è per niente recepito"*[(96)].

3.3 Dalla p.e.c. gratuita al domicilio digitale

Successivamente il legislatore ha introdotto, con la legge n. 69/2009, per le pubbliche amministrazioni regionali e locali, la facoltà di assegnare ai cittadini residenti caselle di posta elettronica certificata per la trasmissione di documentazione ufficiale, senza tuttavia specificarne ulteriormente i dettagli, tale possibilità per le amministrazioni regionali o locali è stata poi, in breve tempo, rimossa con il D.Lgs. 235/2010. Ciò lascia presumere, a parere di chi scrive, che esistano caselle p.e.c. rilasciate ai cittadini da regioni o comuni che non sono necessariamente iscritte negli elenchi di Postacertificat@.

(95) Cit: A.MAZZEO in *[34]*

(96) Rif: A.MAZZEO in *[34]*

Il Decreto Legge 78/2009, convertito con modificazioni dalla L. 102/2009, va ad aggiungere (art. 65 del C.A.D., comma 1 lettera c-bis) tra gli strumenti validi a tutti gli effetti per presentare istanze e dichiarazioni per via telematica alle pubbliche amministrazioni, anche le credenziali di accesso relative all'utenza personale di Postacerticat@, oltre alle già presenti forme di identificazioni come la carta d'identità elettronica o la carta nazionale dei servizi.

Il successivo D.Lg.s. 235/2010 modifica nuovamente il comma 1 lettera c-bis dell'art. 65 rimuovendo lo specifico riferimento alla casella di Postacertificat@ ma dichiarando che sono valide le istanze e le dichiarazioni presentate alle pubbliche amministrazioni se trasmesse dall'autore mediante la propria casella di posta elettronica certificata, purchè le relative credenziali di accesso siano state rilasciate previa identificazione, anche telematica, del titolare e ciò sia attestato, dal gestore del sistema, nel messaggio o in un suo allegato.

L'espressione *"domicilio digitale"* viene utilizzata dal legislatore con l'introduzione dell'art. 3-bis nel Codice dell'Amministrazione Digitale (con l'art. 4 del c.d. *Decreto Crescita 2.0* - D.L. 179/2012 convertito con modificazioni dalla L. 221/2012). La norma offre, a ogni cittadino, la facoltà di indicare alla pubblica amministrazione un proprio domicilio digitale, inteso come un indirizzo di posta elettronica certificata, rilasciato ai sensi dell'art. 16-bis comma 5 del D.L. 185/2008 convertito con modificazioni dalla legge 2/2009, ciò a significare che l'indirizzo p.e.c. che il cittadino potrà indicare è, al momento in cui si scrive, quello fornito attraverso il servizio di Postacertificat@, di cui ampiamente già detto nei paragrafi precedenti.

L'obbligo di utilizzo del domicilio digitale da parte delle pubbliche amministrazioni è corredato di cogenza[(97)]: dal 1° gennaio 2013, dispone il comma 4 dell'art. 3-bis del C.A.D., le pubbliche amministrazioni e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato senza oneri di spedizione a suo carico.

(97) Rif: F.FAINI in *[28]*

Il soggetto pubblico è dunque tenuto a comunicare attraverso essa con delle eccezioni: lo stesso comma 4 dispone che quanto detto vale salvo i casi in cui è prevista dalla normativa vigente una diversa modalità di comunicazione o di pubblicazione in via telematica. *"Un esempio sono l'utilizzo di 'short message service' (o Sms). Si pensi, in concreto, a un Sindaco che abbia necessità di comunicare, tempestivamente, un importante messaggio "di allarme" alla propria comunità locale: egli potrà continuare a utilizzare un più efficace Sms"* [(98)].

Per quanto riguarda conservazione e disponibilità del domicilio digitale, la norma stabilisce che l'indirizzo sia inserito nell'ANPR e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi. Il comma 3 dell'art. 3-bis del C.A.D. dispone, inoltre, che le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino e le modalità di consultazione dell'ANPR, da parte dei gestori o esercenti di pubblici servizi ai fini del reperimento del domicilio digitale dei propri utenti, dovranno essere definite con apposito decreto ministeriale, sentita l'Agenzia per l'Italia digitale.

L'ANPR è attualmente in corso di realizzazione[(99)] e nel D.P.C.M. n. 109 del 23 agosto 2013, ci sono le prime disposizioni attuative in base alle quali la stessa, costituita dall'Indice Nazionale delle Anagrafi (INA) e dall'Anagrafe degli Italiani Residenti all'Estero (AIRE), entro il 31 dicembre 2014 subentrerà alle anagrafi comunali. Con questo regolamento viene avviata la costituzione di questa base di dati di interesse nazionale destinata ad assumere un ruolo strategico nel processo di digitalizzazione della pubblica amministrazione e di miglioramento dei servizi al cittadino, nel quadro dell'Agenda Digitale italiana di cui si dirà più avanti.

---

(98) Cit A.MONEA in *[38]*

(99) Come segnala notizia aggiornata il 20/1/2014 sul sito dell'Agenzia per l'Italia digitale: *http://www.agid.gov.it/identita-digitali/anagrafe-nazionale-popolazione*-residente

Nel D.P.C.M. 109/2013, l’art. 2 comma 2 ribadisce che l’ANPR rende disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi l'indirizzo di posta elettronica certificata indicato dal cittadino quale proprio domicilio digitale, secondo le modalità definite dal decreto ministeriale previsto dall'articolo 3-bis, comma 3, del D.Lgs. n. 82/2005, che deve tuttavia ancora essere predisposto.

Le modalità di accesso all’ANPR, da parte delle P.A. e degli organismi che erogano pubblici servizi, dovranno essere definite attraverso apposite convenzioni (da effettuarsi ai sensi dell’art. 58, comma 2, del C.A.D. in materia di fruibilità dei dati).

Nel D.P.C.M. 109/2013 sono in ogni caso articolate le 3 fasi che dovrebbero portare all’unificazione delle anagrafi:

- fase 1 - fase di attuazione immediata che prevede esclusivamente la modifica dei sistemi di sicurezza mentre restano invariate le modalità di accesso e di trasmissione dei dati;
- fase 2 - fase transitoria che prevede la progressiva migrazione delle banche dati relative alle anagrafi comunali della popolazione residente e dei cittadini italiani residenti all'estero nell'ANPR. In questa fase e' resa disponibile anche la nuova banca dati dell'ANPR contestualmente ai servizi resi dall'INA e dall'AIRE.
- fase 3 - fase definitiva che decorre dal 1° gennaio 2015 in cui l'ANPR subentra alle anagrafi comunali. Effettuata la migrazione delle anagrafi comunali nell'ANPR, le banche dati relative alle anagrafi comunali vengono dismesse.

Il D.L. 21 giugno 2013 n. 69, il c.d. *Decreto del Fare*, convertito con modificazioni dalla L. 98/2013, interviene nuovamente in materia di domicilio digitale, modificando l’art. 10 del D.L. 70/2011. L’art. 10 già tratta, per semplificare il procedimento di rilascio dei documenti obbligatori di identificazione ai cittadini, dell’istituzione del documento unificato che sostituirà la carta di identità, la tessera sanitaria e il tesserino fiscale.

Il D.L. 69/2013 inserisce qui, al comma 3-quater dell'art. 10, l'assegnazione automatica del domicilio digitale: *"All'atto della richiesta del documento unificato, ovvero all'atto dell'iscrizione anagrafica o della dichiarazione di cambio di residenza a partire dall'entrata a regime dell'Anagrafe nazionale della popolazione residente, di cui all'articolo 2 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, è assegnata al cittadino una casella di posta elettronica certificata, di cui all'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, con la funzione di domicilio digitale, ai sensi dell'articolo 3-bis del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, successivamente attivabile in modalità telematica dal medesimo cittadino. Con il decreto del Ministro dell'interno di cui al comma 3 sono stabilite le modalità di rilascio del domicilio digitale all'atto di richiesta del documento unificato"*.

Resta quindi una facoltà, una scelta del cittadino, l'utilizzo di un domicilio digitale (come dispone il comma 1 dell'art. 3-bis del C.A.D.), in quanto, seppure avviene l'assegnazione *d'ufficio* di una casella di posta elettronica certificata, essa sarà, come la norma su riportata dispone, *successivamente attivabile* (o meno) dal cittadino. Pare perciò evidente, a parere di chi scrive, che venga mantenuta la facoltà del cittadino di utilizzare o meno questo canale di comunicazione. Stante l'assegnazione d'ufficio, il vincolo però è posto sulla tipologia di casella, che pare essere unicamente la Postacertificat@ in quanto è, ad oggi, l'unico servizio che consente il rilascio di una casella di posta certificata ai sensi dell'art. 16-bis comma 5 DL. 185/2008. Tutto questo però avverrà dal momento in cui sarà pronta l'Anagrafe Nazionale della Popolazione Residente.

Il legislatore, in ogni caso, con la Legge di conversione n. 98/2013, ha integrato l'art. 3-bis del C.A.D. con i commi 4-bis, ter e quater per le specifiche da seguire, per le pubbliche amministrazioni, in caso di assenza di domicilio digitale. Nel caso il cittadino non disponga di domicilio digitale, le pubbliche amministrazioni possono predisporre le comunicazioni con il soggetto come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia

analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'art. 3 del D.Lgs. 39/1993. Queste disposizioni soddisfano a tutti gli effetti di legge gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente laddove la copia analogica inviata al cittadino contenga una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso la P.A.. Le modalità di predisposizione della copia analogica previste in questa norma soddisfano le condizioni di cui all'art. 23-ter, comma 5, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.

4. La tutela giuridica

Dopo aver trattato, nel secondo capitolo, la valenza giuridica delle trasmissioni via posta elettronica e posta elettronica certificata, si analizzerà ora il tema della tutela dell'indirizzo di posta elettronica, sia esso certificato o meno. Si vedrà come tale indirizzo costituisca un dato personale e, per tale ragione, ad esso si applichino le protezioni previste dal Codice in materia di protezione dei dati personali: l'utilizzazione dell'indirizzo di posta elettronica integra un trattamento dei dati personali del destinatario delle comunicazioni. Si analizzeranno inoltre gli illeciti penali previsti dal legislatore in caso di violazione della corrispondenza informatica. Si trarranno, infine, le conclusioni in merito a quali siano globalmente le tutele ad oggi previste per il domicilio digitale.

4.1 La valenza dell'indirizzo di posta elettronica come dato personale

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla Legge 675/1996 per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali. Con la redazione del Codice in materia di protezione dei dati personali (meglio noto come Codice della Privacy), approvato con il Decreto legislativo n. 196 del 30 giugno 2003, la Legge n. 675/1996 è stata abrogata.

Il Garante si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle loro informazioni personali[(100)].

(100) Sito internet del Garante per la Protezione dei dati personali: *http://www.garanteprivacy.it/*

European Data Protection Supervisor.
ttps://secure.edps.europa.eu/)

Il Garante italiano coopera, assieme agli organi di tutela degli altri paesi europei, con il Garante Europeo per la Protezione dei dati personali (GEPD)[(101)]. Tale autorità di sorveglianza indipendente è nata del 2001 con l'obiettivo primario di garantire che le istituzioni e gli organi dell'UE rispettino il diritto alla vita privata nel trattamento di dati personali soprattutto in sede di elaborazione di nuove politiche.

Il forum centrale per la cooperazione nell'Unione europea è il *Gruppo di lavoro Articolo 29*[(102)], che costituisce il luogo dove le autorità nazionali di protezione dei dati si incontrano per uno scambio di opinioni su temi di attualità, per discutere di una comune interpretazione della legislazione sulla protezione dei dati in quanto la rete ha nel tempo amplificato la circolazione delle informazioni e con essa la necessità di tutelarle.

I dati personali sono tutte quelle informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

I dati personali si distinguono in:

- dati identificativi: quelli che permettono l'identificazione diretta, come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc.;
- dati sensibili: quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;

(101) Rif: *https://secure.edps.europa.eu/EDPSWEB/edps/lang/it/EDPS*

(102) Il Gruppo di lavoro *Articolo 29* è un organo istituito ai sensi dell'art. 29 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
(Rif: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:it:HTML*)

- dati giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche o quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

I dati personali sono costituiti da informazioni esatte e aggiornate, riferite a persone fisiche, identificate o identificabili, che possono essere “trattate” da terzi per finalità legittime, limitate e pertinenti all’uso dovuto.

Per trattamento si intende ogni operazione compiuta, manualmente o con strumenti elettronici, sui dati personali di un individuo.

Il D.Lgs. 196/2003 tutela e disciplina il trattamento di dati personali, anche se detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
La tutela è estesa anche al trattamento dei dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea ed impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea, in questo caso, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

Il trattamento di dati personali effettuato da persone fisiche, per fini esclusivamente personali, è soggetto all'applicazione del Codice in materia di protezione dei dati personali solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione.

In ogni caso si applicano le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli artt. 15 e 31 del suddetto codice[103].

Il trattamento dei dati personali effettuato con strumenti elettronici è consentito solo se sono adottate alcune misure minime previste dall'art. 34:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Tali misure minime devono essere adottate secondo i modi previsti dal disciplinare tecnico che costituisce parte integrante del Codice in materia di protezione dei dati personali[104].

---

[103] Codice in materia di protezione dei dati personali (D.Lgs. 196/2003):

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 (violazione sulle modalità di trattamento e requisiti dei dati).

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

[104] Il disciplinare tecnico, di cui all'allegato B) del Codice in materia di protezione dei dati personali, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore. (Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184*)

I soggetti coinvolti al fine di dare origine al trattamento di dati personali sono:

- l’interessato, è la persona fisica cui si riferiscono i dati personali;
- il titolare, è la persona fisica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., cui spettano le decisioni sugli scopi e sulle modalità del trattamento, oltre che sugli strumenti utilizzati;
- il responsabile, è la persona fisica, la società, l'ente pubblico o privato, l'associazione o l'organismo cui il titolare affida, anche all'esterno della sua struttura organizzativa, specifici e definiti compiti di gestione e controllo del trattamento dei dati. La designazione del responsabile è facoltativa;
- l’incaricato, è la persona fisica che, per conto del titolare, elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare e/o dal responsabile.

L’interessato deve essere informato, oralmente o per iscritto, circa le finalità e le modalità di trattamento dei suoi dati, la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale rifiuto a rispondere; dovrà altresì essere informato sui suoi diritti e sui soggetti o categorie di soggetti che possono venire a conoscenza dei suoi dati. Ha diritto inoltre, ad ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e alla loro comunicazione in forma intelligibile, inoltre può chiedere qual è l’origine dei dati e le modalità, finalità e logica applicate alla loro trattazione. Ha inoltre facoltà di conoscere gli estremi identificativi del titolare e/o dei responsabili, di richiedere l'aggiornamento, la rettificazione, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati stessi se trattati in violazione di legge. L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano anche se pertinenti allo scopo della raccolta; può, inoltre, opporsi al trattamento di dati che lo riguardano ai fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Per l’argomento di interesse, innanzitutto occorre evidenziare che una casella di posta elettronica, sia essa ordinaria o certificata, di una persona fisica è un dato personale e come tale deve essere tutelato.

Uno dei primi pronunciamenti del Garante in materia di posta elettronica risale al 1999[(105)][(106)], quando ha affermato che le e-mail che circolano in internet, seppure nelle liste di posta elettronica e nei newsgroup ad accesso limitato, devono essere considerate come corrispondenza privata e, in quanto tali, non possono essere violate.

La pronuncia è arrivata con riferimento alle e-mail scambiate nell'ambito di una mailing list costituita su iniziativa di alcuni dipendenti di un'amministrazione e con strumenti messi a disposizione dall'amministrazione stessa. Nella sua decisione, il Garante, facendo riferimento all'art. 15 della Costituzione, alla Legge 547/1993 sui reati informatici e al D.P.R. n. 513/1997 sul documento elettronico, ha affermato che la posta elettronica (non solo la singola e-mail ma anche la totalità dei contenuti delle articolate mailing list ovvero i servizi di posta elettronica con un indirizzario automatico che consente la contemporanea trasmissione a più persone di una comunicazione su determinati argomenti di interesse) deve essere tutelata alla stregua della corrispondenza epistolare o telefonica. I messaggi che in esse circolano non possono essere abusivamente intercettati a prescindere dal fatto che la rete operi attraverso le strutture pubbliche che un'amministrazione ha consentito di utilizzare. Nel caso di specie, il Garante ha peraltro precisato che, analogamente a quanto avviene per la normale corrispondenza, non può essere considerata contrastante con la normativa sui dati personali l'eventuale successiva presa di conoscenza della e-mail da parte di soggetti estranei al circuito di posta elettronica, quando il messaggio non sia stato indebitamente acquisito da questi ultimi ma ad essi comunicato da parte di uno dei destinatari del messaggio stesso.

Al di là della specificità di questo pronunciamento che atteneva all'inoltro di una mail, "non troppo gentile" sull'operato della dirigenza, che un dipendente aveva postato sulla mailing list e successivamente un collega si era curato di inoltrare ad un dirigente, la necessità di tutelare le nostre comunicazioni via posta elettronica, ma soprattutto l'esigenza di tutelare il nostro indirizzo di posta elettronica, è un problema molto attuale.

---

(105) Comunicato stampa del Garante per la Protezione dei Dati Personali: *Privacy e posta elettronica* - 12 luglio 1999.
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/47997*)

(106) Rif: C.MORGOGLIONE in *[54]*

Una delle prime cose a cui pensiamo, con riferimento alla nostra casella di posta è che normalmente riceviamo elevate quantità di messaggi indesiderati[(107)].

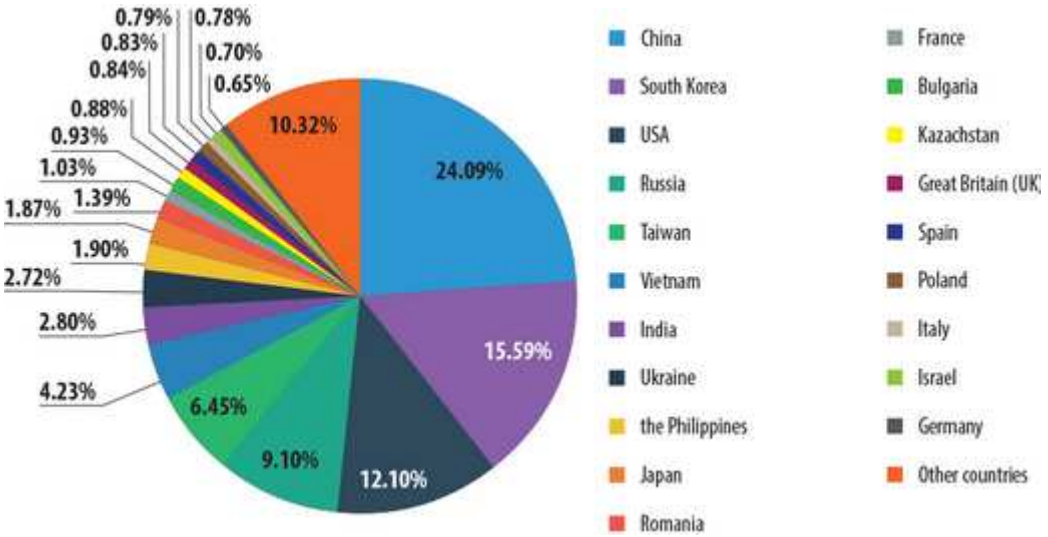
Nella volontà di non addentrarsi, in una più puntuale classificazione dei contenuti malevoli o pubblicitari, occorre dire che, seppure i Server Mail pubblici e i software attuali molto spesso ci consentono di eliminare automaticamente al loro ingresso i messaggi indesiderati o quantomeno di catalogarli all'arrivo in una cartella a parte, in maniera da non disturbare le nostre comunicazioni, l'esigenza di proteggere la nostra casella di posta elettronica da e-mail non desiderate è comunque sempre sentita.

Normalmente, infatti, lasciamo in rete il nostro indirizzo di posta elettronica per tanti e svariati motivi che attengono alla nostra professione, ai nostri interessi, ecc., tuttavia gli indirizzi di posta elettronica non sono liberamente utilizzabili da chiunque per il solo fatto di trovarsi in rete.

La vasta conoscibilità degli indirizzi e-mail che internet consente, non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on-line. Gli indirizzi e-mail non sono "pubblici" come possono essere quelli presenti sugli elenchi telefonici.

---

(107) Dall'analisi di Kaspersky lab, ad Aprile 2014, la quota inerente ai messaggi "spazzatura" rilevati nel traffico globale di posta elettronica era pari al 71,1% del volume complessivo di messaggi e-mail circolanti in Rete.
Sotto è riportata la graduatoria "globale" delle fonti di spam relativa ai paesi dal cui territorio, nel corso del mese di aprile 2014, sono state distribuite in rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura":



(Rif: *http://www.securelist.com/en/analysis/204792336/Spam_in_April_2014*)

In tal senso il Garante per la Privacy ha chiarito che la semplice conoscibilità di fatto di un indirizzo di posta elettronica (non proveniente, quindi, da pubblici registri, elenchi, atti o documenti conoscibili da chiunque) non legittima il titolare del trattamento ad inviare messaggi in assenza del preventivo consenso informato dell'interessato.

L'Autorità ha sottolineato che l'eventuale disponibilità in internet di indirizzi di posta elettronica, anche se resi conoscibili dagli interessati per alcuni specifici scopi (ad esempio un sito personale, aziendale o anche istituzionale), va rapportata alle finalità per cui essi sono pubblicati sulla rete. A maggior ragione questo principio vale in caso di uso indebito di software che rastrellano automaticamente migliaia di indirizzi in rete o li creano "a tavolino" a prescindere da un accertamento sulla loro effettiva esistenza. Per poter inviare e-mail senza violare la privacy degli utenti è obbligatorio, dunque, ottenere prima il loro consenso.

Questo è quanto affermato in uno dei primi pronunciamenti su un ricorso in merito ad attività di spamming[(108)]. Il soggetto ha presentato ricorso in quanto destinatario di un messaggio promozionale non richiesto inviato tramite una e-mail da un'azienda. Il ricorrente lamentava di non aver ricevuto riscontro ad una istanza formulata ai sensi dell'art. 13 della legge n. 675/1996[(109)], con la quale si era opposto al trattamento dei dati che lo riguardano, chiedendo di conoscere la loro origine ed il nominativo dell'eventuale responsabile del trattamento. L'azienda, ribadendo che aveva in ogni caso risposto al ricorrente e che aveva comunque cancellato l'indirizzo di posta elettronica dagli archivi della società, aveva sostenuto che il trattamento effettuato fosse lecito in quanto riferito a dati rinvenuti su una pagina web nella quale l'interessato li

---

(108) Garante per la protezione dei dati personali – *Pronunciamento su ricorso: reti telematiche e Internet - Spamming su indirizzo di docente universitario* - 25 luglio 2002
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1065978*)

(109) Il Codice in materia di protezione dei dati personali a cui si riferisce è la Legge 675/1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. All'art. 13 venivano riportati i diritti dell'interessato in relazione al trattamento di dati personali tra cui era compreso il diritto di ottenere, a cura del titolare o del responsabile, senza ritardo, la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento.
La Legge n. 675/1996 è stata successivamente abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia dei dati personali (D.Lgs. 30 giugno 2003, n. 196) che lo ha sostituito. All'art. 7 del D.Lgs. 196/2003 sono confermati i medesimi diritti riconosciuti all'interessato.

avrebbe pubblicati ponendoli "a disposizione degli utenti internet che vi hanno libero accesso". Il Garante osserva che l'interessato non ha fornito il consenso e non sussiste neppure alcuno dei presupposti al trattamento di cui all'art. 12 della L. n. 675/1996 (casi di esclusione del consenso), all'art. 10 del D. lg. 13 maggio 1998, n. 171 o all'art. 10 del d. lg. 22 maggio 1999, n. 185, in materia di contratti a distanza. Contrariamente a quanto sostenuto dall'azienda, la ricerca e il successivo utilizzo dell'indirizzo di posta elettronica del ricorrente ha dato luogo ad un trattamento di dati personali. Il Garante ha ribadito che la disponibilità in Internet degli indirizzi di posta elettronica resi conoscibili attraverso siti web va rapportata alle finalità per cui essa è avvenuta a cura dei soggetti che curano tali siti. I dati personali resi in tal modo conoscibili in relazione ad eventi e delimitate finalità non sono inoltre liberamente utilizzabili per l'invio generalizzato di e-mail aventi contenuto commerciale o pubblicitario. Nel caso di specie, nel precisare che chiunque, essendovi tenuto, non osservi un provvedimento adottato dal Garante, è punito con la reclusione da tre mesi a due anni, l'azienda è stata condannata a comunicare gli estremi identificativi dei responsabili del trattamento eventualmente designati.

Si citerà ora un ricorso relativo all'invio di mail indesiderate in materia di comunicazione politica[(110)]. L'11 gennaio 2001 con riferimento alle comunicazioni indesiderate in materia di propaganda elettorale, il Garante comunica di aver avviato accertamenti nei confronti di un'associazione politica ai fini della verifica della liceità e correttezza di alcuni trattamenti di dati relativi ad indirizzi di posta elettronica, in relazione a circa trenta segnalazioni che lamentavano la ricezione, non gradita, di messaggi per via telematica da una associazione per finalità di comunicazione politica. Diversi cittadini lamentavano anche di aver ricevuto numerosi messaggi dal medesimo contenuto in un arco ravvicinato di tempo. Altri hanno fatto invece presente che non era stato loro possibile cancellarsi dagli elenchi dei destinatari secondo le modalità indicate nelle e-mail non gradite, o di essere stati costretti a reiterare invano più richieste di cancellazione.

---

(110) Garante per la protezione dei dati personali – *Reti telematiche e Internet - Prescrizioni e divieto del Garante - Comunicazione politica, e-mail, atti e documenti pubblici conoscibili da chiunque* - 11 gennaio 2001. (Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/40823*)

L'associazione dichiarava espressamente di aver reperito oltre 390.000 indirizzi di posta elettronica a scopo di comunicazione politica, utilizzando un software a disposizione di un terzo, il quale avrebbe archiviato indirizzi e-mail visualizzati su pagine web con suffissi ".it", ".org", ".com" e ".net" accessibili a chiunque in rete senza l'uso di password o di altri sistemi di protezione.

Stante che la circostanza non ha trovato pieno riscontro in quanto, da accertamenti tecnici effettuati, in almeno otto casi non è stato possibile reperire in rete gli indirizzi di posta elettronica dei cittadini che hanno inviato una segnalazione, questo aspetto non si ritiene rilevante. Infatti, anche dando per assunto che pure questi otto indirizzi siano stati effettivamente raccolti mediante il software menzionato dall'associazione, l'utilizzazione per finalità di comunicazione politica di tali indirizzi, e degli altri che sono stati invece reperiti in rete, non risulta comunque lecita e corretta.

Contrariamente a quanto argomentato dall'associazione, gli indirizzi di posta elettronica dei segnalanti non provengono da "pubblici registri, elenchi, atti o documenti conoscibili da chiunque" e la loro utilizzazione nel caso in esame non è quindi consentita in mancanza di una previa manifestazione positiva di consenso da parte degli interessati (art. 12 della legge n. 675/1996).

Non è possibile utilizzare liberamente qualsiasi dato personale di natura non sensibile in base alla sola circostanza che il dato sia stato conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti.

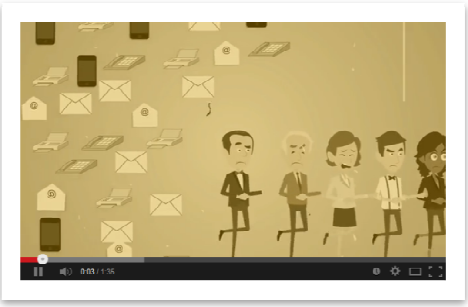
L'utilizzazione per finalità di comunicazione politica degli indirizzi di posta elettronica dei segnalanti non poteva pertanto avvenire senza un preventivo consenso manifestato dagli interessati. Per nessuno dei cittadini che ha presentato la segnalazione è invece risultato dimostrato che l'interessato abbia espresso il proprio consenso alla divulgazione e all'utilizzazione da parte di chiunque del proprio indirizzo di posta elettronica. É parimenti per un verso infondata e per un altro ininfluente la tesi secondo cui, con la partecipazione a forum e newsgroup, l'utente "decide di pubblicare (cioè di rendere pubblico) il proprio indirizzo di posta elettronica" ed "è consapevole che quell'indirizzo, quel dato, potrà esser letto ed acquisito da chiunque si trovi 'a passare' dalla pagina web interessata". Va considerato infatti che la conoscenza di fatto degli indirizzi che si realizza in tali casi non può essere disgiunta dalla finalità per cui essa avviene.

Contrasta, pertanto, con i principi di correttezza e finalità del trattamento raccogliere i dati che singoli utenti “lasciano” in un newsgroup, forum, ecc. solo per le finalità di specifica discussione su determinati temi, hobbies, ecc., ed utilizzarli per altri scopi che nulla hanno a che vedere, anche indirettamente, con l'argomento per il quale l'utente partecipa ad una discussione più o meno “pubblica” ed indica il proprio recapito e le proprie generalità.

Ad una conclusione, analoga a quella indicata, deve pervenirsi anche per ciò che riguarda altri casi oggetto di segnalazione, nei quali gli indirizzi di posta elettronica sono stati acquisiti dall'associazione in quanto pubblicati su alcuni siti web per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale ed associativa: la pubblicità di alcuni indirizzi resi conoscibili attraverso tali siti va collegata anch'essa, infatti, agli scopi per cui essa si verifica, non potendosi sostenere, anche in tali casi, che i dati posti a disposizione del pubblico per circoscritte finalità siano liberamente utilizzabili per l'invio generalizzato di e-mail anche quando queste non abbiano un contenuto commerciale o pubblicitario.

Le segnalazioni sono infine fondate anche per ciò che riguarda le modalità di cancellazione dei dati in quanto a prescindere dalla liceità o meno della loro utilizzazione, l'associazione era tenuta a soddisfare senza ritardo le richieste di cancellazione ai sensi dell'art. 13 della legge n. 675/1996, curando un servizio attivo ed efficace di eliminazione degli indirizzi dei reclamanti. Il numero delle segnalazioni pervenute al riguardo (che lamentano l'inerzia dell'associazione o l'inattività del meccanismo telematico predisposto) non sembra invece far ritenere che si sia trattato solo di un disguido occasionale.

L'associazione è così condannata ad astenersi dall'utilizzare ulteriormente i dati personali relativi agli utenti che non abbiano previamente manifestato un consenso alla loro utilizzazione per finalità di comunicazione politica e deve adottare inoltre ulteriori misure per dare effettivo seguito alle richieste di cancellazione dei dati già pervenute o che pervengano successivamente.



Fotogramma estratto del video per la campagna informativa*:"Spam. I consigli del Garante privacy per difendersi"* pubblicato il 10/09/2013 su *www.garanteprivacy.it/spam.*

Il Garante ha messo in atto diverse campagne di comunicazione volte a sensibilizzare il pubblico su tematiche specifiche relative al trattamento dei dati personali che utilizzano diverse tipologie di prodotti di comunicazione legati molto spesso all'uso di strumenti informatici[(111)], come ad esempio *"Spam: come difendersi"* nel 2013.

Nello stesso anno il Garante ha pubblicato le *Linee guida in materia di attività promozionale e contrasto allo spam*[(112)].

Le Linee guida ribadiscono che non è possibile effettuare attività di marketing diretto se non si è acquisito il consenso preventivo e informato del soggetto (il c.d. *opt-in*), in quanto, non è lecito presumere l'accettazione di una comunicazione per il solo fatto che la casella di posta elettronica è presente su liste d'indirizzi, siti web o altre fonti di pubblico dominio. Le informazioni che riguardano le modalità di trattamento dei dati, le finalità e i canali usati, devono inoltre essere sempre fornite prima della comunicazione commerciale e per questo motivo non è lecito informare l'utente contestualmente con l'invio di una comunicazione commerciale, chiedendo eventualmente allo stesso di dare o negare il consenso per i successivi invii.

Sebbene il principio generale sia quello che non è possibile sfruttare la stessa espressione di consenso per scopi diversi, il Garante ha comunque stabilito che l'invio di pubblicità, vendita diretta, ricerche di mercato e simili possano essere ricondotte a una stessa iniziativa di marketing per cui può valere un'unica manifestazione di consenso. Se invece i dati raccolti servono per creare liste profilate per generare altre comunicazioni o per la cessione a terzi, allora è necessario ottenere espressioni di consenso per ogni specifico utilizzo.

---

(111) Garante la Protezione dei Dati Personali: *Campagne di comunicazione istituzionale.* (Rif: *http://www.garanteprivacy.it/home/stampa-comunicazione/campagne-di-comunicazione-istituzionale*)

(112) Garante la Protezione dei Dati Personali: *Linee guida in materia di attività promozionale e contrasto allo spam* - 4 luglio 2013. Registro dei provvedimenti n. 330 del 4 luglio 2013. (Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348)*

E’ consentito inviare, senza alcun consenso preventivo, e-mail promozionali a persone che hanno comunicato la propria casella nel contesto di precedenti acquisti ma sono vietate le proposte di merci o servizi diversi da quanto già acquistato, a meno che l’interessato non sia stato informato e abbia dato il suo consenso. Infine per quanto riguarda le comunicazioni agli indirizzi, acquisiti sui social network, vieta l’impiego dei dati presenti nei profili personali per l’invio di messaggi promozionali in assenza di un consenso specificamente espresso. Considera invece come *assunta* l’esplicita espressione di consenso all’invio di materiale promozionale se vi è stata l’adesione alla c.d. *fan-page* di una società o di un marchio o prodotto commerciale[(113)].

Il pronunciamento del Garante che ora si analizza è del 6.5.2013 e si esplicita in un divieto al trattamento di dati personali contenuti in corrispondenza privata acquisita illecitamente[(114)]. Il Garante, avendo ricevuto informazioni secondo le quali l'intero contenuto di numerose mail appartenenti a deputati di un partito politico, sarebbe stato pubblicato sulla rete e, stante la questione sollevata da una delegazione di parlamentari del medesimo partito direttamente negli uffici dell'Autorità, ha rilevato l'effettiva reperibilità sulla rete internet di e-mail riconducibili a taluni deputati del partito.

L'attività descritta configura innanzitutto la violazione di un diritto fondamentale tutelato dall'art. 15 della Costituzione, a garanzia dell'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, anche in considerazione delle particolari garanzie poste dall'art. 68 della Costituzione[(115)] a tutela delle comunicazioni e della corrispondenza dei membri del Parlamento; inoltre, la vicenda potrà determinare responsabilità di natura penale e assumere rilievo anche sotto

---

(113) Rif.: P.TODOROVICH in *[42]*

(114) Garante per la protezione dei dati personali – *Divieto del trattamento di dati personali contenuti in corrispondenza privata acquisita illecitamente* - 6 maggio 2013
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2411368

(115) L’art. 68 della Costituzione dispone: *“I membri del Parlamento non possono essere chiamati a rispondere delle opinioni espresse e dei voti dati nell'esercizio delle loro funzioni. Senza autorizzazione della Camera alla quale appartiene, nessun membro del Parlamento può essere sottoposto a perquisizione personale o domiciliare, né può essere arrestato o altrimenti privato della libertà personale, o mantenuto in detenzione, salvo che in esecuzione di una sentenza irrevocabile di condanna, ovvero se sia colto nell'atto di commettere un delitto per il quale è previsto l'arresto obbligatorio in flagranza. Analoga autorizzazione è richiesta per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza.”*

il profilo della vigente disciplina in materia di protezione dei dati personali, configurandosi quale trattamento di dati riferibili a persone identificate. Il trattamento è da ritenersi illecito in quanto avvenuto in violazione della legge ed in particolare dell'art.11 comma 1, lett. a) e b)[116] del D.Lgs. 196/2003.

La vicenda è consistita nell'acquisizione e nella diffusione di dati personali all'insaputa e contro la volontà degli interessati. Tale violazione, secondo il Garante, determina una lesione del diritto alla riservatezza e alla protezione dei dati personali, non solo dei parlamentari intestatari degli indirizzi di posta elettronica, ma di tutti coloro che sono entrati in contatto con essi via e-mail, nonché eventualmente di terzi citati all'interno delle comunicazioni. Inoltre, l'illiceità *ab origine* del trattamento di dati personali estende i suoi effetti anche ad eventuali successivi trattamenti, rendendo così illecita ogni altra successiva operazione di raccolta, conservazione e ulteriore utilizzo dei medesimi dati ai sensi dell'art. 11 comma 2 del D.Lgs. 196/2003.

Il Garante ha ritenuto pertanto necessario disporre, ai sensi degli artt. 143 lett. c) e 154 comma 1 lett. d)[117] del codice, il divieto ad ogni eventuale ulteriore trattamento delle e-mail dei deputati diffuse sulla rete con conseguente obbligo, in capo a chi le detenga, di provvedere alla loro cancellazione.

---

(116) D.Lgs. 30 giugno 2003, n. 196 - Art. 11. *Modalità del trattamento e requisiti dei dati*

1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

(117) Ai sensi dell'art. 143 lett. c) e dell'art. 154 lett. d) del D.Lgs. 30 giugno 2003, n. 196, il Garante può disporre il divieto al trattamento che risulti illecito o non corretto anche per effetto della mancata adozione delle misure necessarie per rendere il trattamento conforme alle disposizioni vigenti.

Il Garante ha altresì ricordato che, in caso di inosservanza del provvedimento, si renderanno applicabili le sanzioni previste agli artt. 162[(118)] comma 2-ter e 170[(119)] del D.Lgs. 196/2003. In ogni caso avverso ogni provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria con ricorso depositato al tribunale del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

4.2 Il Garante e la tutela dei dati personali nella P.A.

La tutela dei dati personali è naturalmente riconosciuta anche quando colui che tratta i dati è una pubblica amministrazione alla quale in linea generale si applica il disposto dell'art. 18 del D.Lgs. 196/2003, dove viene innanzitutto stabilito che qualunque trattamento di dati personali da parte di soggetti pubblici (ad esclusione degli enti pubblici economici) è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Nel trattare i dati, il soggetto pubblico osserva i presupposti e i limiti stabiliti per i trattamenti dal D.Lgs. 196/2003 stesso, anche in relazione alla diversa natura dei dati,

---

(118) D.Lgs. 30 giugno 2003, n. 196 - Art. 162. *Altre fattispecie*

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro.

2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da mille euro a seimila euro.

2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta

2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.

2-quater. La violazione del diritto di opposizione nelle forme previste dall'articolo 130, comma 3- bis, e dal relativo regolamento è sanzionata ai sensi del comma 2-bis del presente articolo.

(119) D.Lgs. 30 giugno 2003, n. 196 - Art. 170. *Inosservanza di provvedimenti del Garante*

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

nonchè dalla legge e dai regolamenti. A meno che non si tratti di esercenti le professioni sanitarie e di organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

Le pubbliche amministrazioni sono comunque sottoposte alle limitazioni in tema di comunicazione e diffusione da quanto stabilito dall'art. 25[(120)].

L'art. 19 afferma che il trattamento da parte di un soggetto pubblico, riguardante dati diversi da quelli sensibili e giudiziari, come è appunto un indirizzo di posta elettronica, è consentito soltanto per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata. Infine la comunicazione e la diffusione da parte di un soggetto pubblico a privati o ad enti pubblici economici sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

---

(120) D.Lgs. 30 giugno 2003, n. 196 - Art. 25. *Divieti di comunicazione e diffusione*

1. *La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:*
   a) *in riferimento a dati personali dei quali e' stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e);* (cioè è decorso il tempo necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati)
   b) *per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.*
2. *E' fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.*

Si riporta un pronunciamento del Garante in materia di diritto di accesso[(121)].

Il ricorrente, dipendente di un'unità sanitaria locale lamenta di non aver ricevuto positivo riscontro alla richiesta avanzata ai sensi dell'art. 13 della legge n. 675/1996, riferita al complesso dei propri dati personali detenuti dal predetto datore di lavoro. L'unità sanitaria ha fornito al Garante copia della risposta inviata all'interessato dove viene indicato il diniego all'accesso ai dati personali ai sensi del citato art. 13 ritenendo che, se esercitato nei confronti di un "organismo a rilevanza pubblica", il diritto di accesso ai dati incontrerebbe un limite di riservatezza "in ordine ad elementi che si inseriscono in un procedimento finalizzato al perseguimento di interessi pubblici".

L'accesso ai dati, in altre parole, secondo l'unità sanitaria locale, dovrebbe essere contemperato con "l'interesse pubblicistico alla riservatezza degli atti interni di un procedimento amministrativo".

Il Garante ha affermato che il diritto di accedere ai dati personali del richiedente è esercitabile nei confronti di qualsiasi titolare del trattamento pubblico e privato e non è soggetto alle limitazioni ipotizzate dall'Azienda Sanitaria Locale. Gli unici limiti all'esercizio del diritto di cui all'art. 13 sono previsti dall'art. 14 della medesima legge n. 675/1996, che prevede altre esclusioni per particolari categorie di titolari del trattamento o per specifiche ipotesi espressamente individuate fra le quali non rientra quella oggetto di eccezione. In conseguenza di ciò il Garante, nell'accogliere il ricorso, ordina all'Azienda Unità Sanitaria di comunicare all'interessato i dati personali che lo riguardano.

Il diritto di accesso ai dati personali può essere esercitato nei confronti di un titolare del trattamento sia pubblico, sia privato, e non è soggetto ai limiti posti dalla legge per l'accesso ai documenti amministrativi.

---

(121) Garante per la protezione dei dati personali – *Diritto di accesso - L'interessato può accedere ai dati personali anche quando il titolare è soggetto pubblico*, 31 gennaio 2002
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1064233*)

Stante quanto sino ad ora detto, sono comunque molteplici le sfaccettature legate al trattamento del dato personale *casella di posta elettronica* da parte delle pubbliche amministrazioni, in tal senso alcuni recenti pronunciamenti del Garante pongono in evidenza alcune nuove problematiche legate alla necessità per le P.A., da un lato di attenersi alle recenti norme in materia di trasparenza dell'attività amministrativa che prevedono obblighi di pubblicazione sul sito web istituzionale delle informazioni previste dal D.Lgs. 14 marzo 2013, n. 33 *("Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"),* dall'altro di fornire adeguate garanzie alla tutela dei dati personali.

Il 15 maggio 2014 il Garante ha emanato le *"Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"*[(122)] al fine di definire un quadro unitario di misure e accorgimenti volti a individuare opportune cautele che i soggetti pubblici, e gli altri soggetti parimenti destinatari delle norme vigenti, sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa. Tale provvedimento sostituisce le precedenti linee in materia del 2 marzo 2011.

Secondo queste Linee guida recentemente approvate, le P.A. devono pubblicare solo dati esatti, aggiornati e contestualizzati; inoltre, prima di mettere on-line sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali, le amministrazioni devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo. Se le P.A. intendono pubblicare dati personali ulteriori rispetto a quelli individuati nel D.L.gs. 33/2013, devono procedere prima all'anonimizzazione di questi dati, evitando soluzioni che consentano l'identificazione, anche indiretta o a posteriori, dell'interessato.

---

(122) Garante per la protezione dei dati personali – *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* - Registro dei provvedimenti n. 243 del 15 maggio 2014
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436#linee*)

Nelle linee guida viene evidenziata inoltre la necessità di pubblicazione di dati pertinenti e non eccedenti, ad esempio, con riguardo alla pubblicità degli esiti di prove concorsuali o graduatorie, non possono formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (come l'indirizzo di posta elettronica). Inoltre viene ulteriormente ricordato che è illecito, ad esempio, riutilizzare a fini di marketing o di propaganda elettorale i recapiti e gli indirizzi di posta elettronica del personale della P.A. oggetto di pubblicazione obbligatoria, in quanto tale ulteriore trattamento deve ritenersi incompatibile con le originarie finalità di trasparenza per le quali i dati sono resi pubblicamente disponibili. Lo scopo perseguito dalle disposizioni che impongono la pubblicazione dei dati del personale, infatti, seppure non espressamente indicato, è quello di aiutare ad individuare i soggetti e i recapiti da contattare per presentare istanze o ottenere informazioni relative a procedimenti di competenza delle pubbliche amministrazioni (es. il responsabile del procedimento nel D.Lgs. n. 33/2013).

Il Garante, con riferimento alla posta elettronica certificata, ha espresso parere favorevole sullo schema di provvedimento richiesto da DigitPa recante regole tecniche volte a disciplinare le modalità di consultazione ed estrazione di indirizzi e di elenchi di indirizzi di posta elettronica certificata, da parte delle pubbliche amministrazioni, di cui agli artt. 16 comma 10 e 16-*bis* comma 5 del D.L. n. 185/2008, convertito con modificazioni dalla Legge n. 2/2009[(123)]. Il parere favorevole è stato emesso dopo il recepimento, da parte di DigitPa, degli aspetti relativi:

- all'effettiva osservanza dei principi di finalità e pertinenza dei dati trattati di cui all'art. 11, comma 1, lettere b) e c) del Codice in materia di protezione dei dati personali;
- all'esatta delimitazione della sfera soggettiva e oggettiva di applicazione del provvedimento;
- alle modalità di realizzazione del flusso informativo tra i soggetti coinvolti e agli obblighi cui questi ultimi sono tenuti;

[(123)] Garante per la protezione dei dati personali - *DigitPA: regole tecniche per la consultazione ed estrazione di indirizzi e di elenchi di indirizzi di posta elettronica certificata (PEC) di cittadini, imprese e professionisti, da parte della pubblica amministrazione*. Registro dei provvedimenti n. 151 del 21 aprile 2011 (Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1807547*)

- alle misure di sicurezza necessarie e in particolare al tracciamento delle richieste di accesso e delle operazioni eseguite.

Tali regole tecniche, per la consultazione ed estrazione di indirizzi p.e.c. ed elenchi di indirizzi p.e.c. di cui all'art. 6 comma 1-bis del C.A.D., ottenuto il parere favorevole del Garante, sono state emanate da DigitPA il 22 Aprile 2011[(124)]. Tale disposizione che regolamenta le modalità di consultazione degli indirizzi P.E.C. di cittadini, imprese e professionisti e di estrazione degli elenchi dei medesimi indirizzi, acquisisce particolarmente rilevanza in quanto consente alle P.A. di accedere a tali informazioni.

In merito alla protezione del dato personale *domicilio digitale*, essendo in ogni caso un indirizzo di posta elettronica, ad esso dovranno certamente applicarsi tutte le tutele su dette. Inoltre, trattandosi di un indirizzo di posta elettronica certificata rilasciato ai sensi dell'art. 16-bis comma 5 del D.L. 185/2008, ad esso si applicano le ulteriori tutele previste in materia di consultazione da parte delle P.A..

Il servizio di Postacertificat@, ad oggi, fornisce sul suo sito[(125)] indicazioni in merito alle modalità con cui le pubbliche amministrazioni possono consultare gli indirizzari centralizzati dei cittadini e delle P.A. che dispongono di una casella di Postacertificat@.

Stante che il domicilio digitale troverà collocazione nell'A.N.P.R., il Garante, in data 24 aprile 2013, ha espresso il parere di competenza[(126)] su uno schema di decreto recante disposizioni "di prima attuazione" dell'A.N.P.R. (art. 62 C.A.D.). Tale schema precisava che con successivi decreti (da adottarsi ai sensi del medesimo art. 62, comma 6 C.A.D.), si sarebbero disciplinate le ulteriori modalità di attuazione della disposizione normativa in questione, anche con riferimento al subentro dell'A.N.P.R. alle Anagrafi

---

(124) Le regole tecniche per la consultazione ed estrazione di indirizzi PEC ed elenchi di indirizzi PEC di cui all'art. 6 comma 1-bis del CAD sono disponibili all'indirizzo:
http://archivio.digitpa.gov.it/sites/default/files/Regole_tecniche _estrazione_PEC_rev_AGDP_4-2.pdf

(125) Postacertificat@, Indirizzari Cittadini e Pubblica Amministrazione
(Rif: *https://www.postacertificata. gov.it/guida_pa/accesso-agli-indirizzari-cittadini-e-pa.dot*)

(126) *Parere del Garante su uno schema di decreto recante disposizioni per la prima applicazione dell'articolo 62 del decreto legislativo 82/2005, che istituisce presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente - 24 aprile 2013.* Registro dei provvedimenti n. 216 del 24 aprile 2013 (Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2448700*)

Comunali, alle relative misure di sicurezza e alle specifiche tecniche concernenti l'organizzazione e il flusso dei dati. Il Garante, nell'esprimere il parere sullo schema, si era riservato di valutare i sistemi e le misure di sicurezza relativi alle successive fasi del progetto di attuazione. Lo schema del decreto, poi approvato, è divenuto il D.P.C.M. 23 agosto 2013, n. 109. Un più recente parere[(127)], richiesto al Garante, su uno schema di regolamento in materia di Anagrafe Nazionale della Popolazione Residente, non tratta la specificità del domicilio digitale.

4.3 La tutela penale della corrispondenza

La casella di posta elettronica costituisce indubbiamente un contenitore di *files*. Il legislatore ha, ormai da oltre un ventennio, equiparato le e-mail alla classica corrispondenza epistolare. La tutela della corrispondenza ed in particolare la libertà e la segretezza delle comunicazioni sono un diritto fondamentale riconosciuto a livello costituzionale.

L'art. 15 della Costituzione ne dispone la riserva di legge e di giurisdizione: *"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."*

L'art. 616 del Codice Penale dispone i termini della violazione e la pena prevista: *"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".*

---

(127) *Parere del Garante su uno schema di regolamento in materia di Anagrafe Nazionale della Popolazione Residente - 17 aprile 2014.* Registro dei provvedimenti n. 202 del 17 aprile 2014
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3105794*)

Con riferimento alla corrispondenza cartacea *chiusa*, imbustata e sigillata come una lettera, sussiste quindi la protezione contro le intrusioni che si concretizzano con la violazione della riservatezza della corrispondenza in sé per sé considerata, sia attraverso condotte consistenti nel prendere conoscenza del contenuto, sia attraverso condotte di rivelazione del contenuto, sia attraverso condotte volte alla distruzione della corrispondenza stessa; condotte tra loro diverse ma che sono comunque punibili secondo l'art. 616 del c.p.[(128)]. Per la corrispondenza c.d. *aperta*, come una cartolina, non è punibile la semplice "presa di cognizione" ma lo sono ovviamente l'eventuale sottrazione al destinatario ovvero la distrazione dalla sua destinazione.

La Legge 547/1993 *("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica")* con lo scopo di adeguare il Codice Penale alla progressiva diffusione delle tecnologie informatiche nelle comunicazioni, ha esteso la tutela penale attribuita alla corrispondenza tradizionale anche alla posta elettronica. L'art. 5 della Legge 547/1993 ha aggiunto infatti, all'art. 616 c.p., il comma 4: *"Agli effetti delle disposizioni di questa sezione, per 'corrispondenza' si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza"*.

La specificazione di corrispondenza *chiusa*, al primo comma dell'art. 616 c.p., assume particolare rilevanza in merito alla tutela delle comunicazioni via posta elettronica. Stante che le e-mail, per loro natura, sono corrispondenza chiusa in quanto sono protette da una password, si deve ritenere che la corrispondenza contenuta nella casella sia conoscibile solo da parte del soggetto che legittimamente dispone di tale password di accesso. Il contenuto di una e-mail può essere letto solo dal legittimo destinatario, essendo essa parificata a tutti gli effetti, anche penali, alla corrispondenza epistolare. Per tale ragione, alle violazioni effettuate sul contenuto di una casella di posta elettronica da parte di persone non autorizzate, si applicherà l'art. 616 c.p. sulla violazione della corrispondenza.

---

(128) Rif: E.BASSOLI, pagg. 221-224 in *[40]*

Tuttavia, stante la *chiusura del contenuto delle e-mail*, di cui appena detto, si ritiene interessante riportare un pronunciamento della Corte di Cassazione[(129)] in merito alla lecita conoscibilità o meno, da parte del datore di lavoro o superiore gerarchico, della corrispondenza via e-mail in partenza o in arrivo sulla casella di posta elettronica del lavoratore. Nella fattispecie infatti, il datore di lavoro era stato imputato del reato di cui all'art. 616 c.p. per avere preso visione del contenuto della corrispondenza di una dipendente, previa utilizzazione della password posta a protezione della stessa.

La Cassazione ha affermato, sul presupposto di diritto che la condotta di cognizione dell'altrui corrispondenza, non sottratta né distratta dalla sua destinazione, è punibile solo se riguardi corrispondenza chiusa, tuttavia non può considerarsi quale corrispondenza chiusa quella accessibile da parte di tutti coloro che legittimamente dispongano della "chiave informatica di accesso". E tra tali soggetti legittimati, ha precisato la Corte, rientra indubbiamente anche il dirigente d'azienda laddove, come nel caso di specie, le password di accesso ai computer e alla corrispondenza di ciascun dipendente siano a conoscenza dell'organizzazione aziendale per essere state comunicate, sia pure in busta chiusa, al superiore gerarchico, legittimato quindi a utilizzarle anche per la mera assenza dell'utilizzatore abituale.

Sull'argomento, il Garante per protezione dei dati personali, dal canto suo, "*visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici"* ha disposto le *Linee guida per posta elettronica e internet* con delibera n. 13/2007 con le quali ha ritenuto necessario fornire indicazioni in tal senso dato che "*è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet"* [(130)] .

---

(129) Quinta Sezione Penale della Corte di Cassazione: Sentenza n. 47096 dell'11.12. 2007. *Delitti contro la persona – violazione di corrispondenza informatica - utilizzazione della password – conseguenze* (Rif: *http://www.cortedicassazione.it/Documenti/47096sen_07.htm*)

(130) Cit: Garante per la Protezione dei Dati Personali: Lavoro*: le linee guida del Garante per posta elettronica e internet*, Registro delle deliberazioni n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007.
(Rif: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522*)

Riprendendo, al di là di questa specificità, la trattazione delle condotte incriminanti previste dall'art. 616 c.p. con riferimento alla posta elettronica, esse sono certamente la *violazione* e la *rivelazione* del contenuto dell'e-mail da parte di un estraneo. Si tratta ad esempio del caso in cui, un soggetto, essendosi indebitamente procurato le credenziali di accesso attraverso tecniche fraudolente, è riuscito ad accedere ad una casella di posta elettronica senza esserne legittimato e, dopo averne preso visione, ne abbia eventualmente rivelato il contenuto ad estranei. La *distrazione* della corrispondenza invece, si concretizza in azioni, come l'utilizzo di appositi software o dispositivi fisici, che consentano di deviare l'e-mail verso destinazioni diverse dalla casella del legittimo destinatario. La *soppressione* consiste nella distruzione o nell'occultamento dell'e-mail, in maniera da renderla comunque irreperibile al destinatario.

Con l'art. 4 della legge 547/1993 il legislatore ha introdotto nel Codice Penale un insieme di reati in materia di criminalità informatica che possono essere posti in essere accanto alla violazione di corrispondenza informatica.

Accade infatti che, in maniera concomitante al reato di cui all'art. 616 c.p., si configurino altri reati che possono essere connessi alle modalità utilizzate per giungere alle condotte di violazione di corrispondenza informatica. In particolare si ricordano il reato di: *"Accesso abusivo ad un sistema informatico o telematico"*[(130)], *"Detenzione e*

---

(130) Art. 615-ter c.p. - *Accesso abusivo ad un sistema informatico o telematico*
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

diffusione abusiva di codici di accesso a sistemi informatici o telematici"[131] e "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico"*[132]. Dove la condotta tenuta abbia consentito di raggiungere un profitto con l'altrui danno, si potrebbe configurare anche il reato di "*Frode informatica"*[133].

---

[131] Art. 615-quater c.p - *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*.
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.
In quest'ultimo comma si stabilisce il raddoppio della pena se il danno è arrecato ad un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, oppure se il soggetto che ha compiuto la violazione è un pubblico ufficiale o un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

[132] Art. 615-quinquies c.p. - *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*
Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

[133] Art. 640-ter c.p. - *Frode informatica.*
Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
Il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante.

L’art. 6 della Legge 547/1993 ha introdotto nel Codice penale anche la tutela penale delle azioni volte ad attuare intercettazioni telematiche o interferenze illecite.

I bit di cui è composta una e-mail, nel momento in cui attraversano la rete (per raggiungere il server di posta o perché dal server raggiungono il destinatario) possono essere intercettati, cioè raccolti, oppure danneggiati da un estraneo *“in ascolto fraudolento”* in tal caso si possono configurare i reati di “*Intercettazione, impedimento o interruzione illecita di comunicazioni”*[134], se ciò avviene attraverso apparati fisici potremmo essere nel caso di *“Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche”*[135]. Se infine le intercettazioni si trasformano in alterazione o distruzione della trasmissione di bit si potrebbe trattare anche di *“Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche”*[136].

---

[134] Art. 617-quater c.p. - *Intercettazione, impedimento o interruzione illecita di comunicazioni*
Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato.

[135] Art. 617-quinquies c.p. - *Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.*
Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

[136] Art. 617-sexies c.p. - *Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.*
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

In tal senso una sentenza della Corte di Cassazione del 2012[(137)] va a delineare bene cosa si debba intendere per domicilio informatico.

Il ricorso, peraltro accolto, è stato effettuato dal legale rappresentante di una società contro un ex dipendente, reo di aver violato il server di posta elettronica di cui la stessa società è titolare. In particolare il soggetto, avendo lavorato per alcuni anni come responsabile dell'ufficio del personale con mansioni di tecnico informatico e conoscendo gli indirizzi e-mail degli impiegati, si era introdotto abusivamente nel server di posta elettronica della società effettuando, da casa, molti tentativi di violazione di accesso a caselle e-mail di membri della società, alcuni dei quali giunti a buon fine, violando molti account dei dipendenti e trasmettendo altresì e-mail destinate al servizio di posta elettronica interna mediante gli account violati.

I motivi dell'accoglimento si basano sull'art. 615-ter c.p. e sulle intenzioni del legislatore, interpretate dalla Corte, di assicurare nella sezione del Codice penale dedicata ai delitti contro la inviolabilità del domicilio, la tutela al *domicilio informatico*, inteso quale spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici di pertinenza della persona, estendendo ad esso la tutela della riservatezza della sfera individuale, quale bene protetto anche costituzionalmente.

La Cassazione, dà una ulteriore lettura dell'art. 615-ter, andando ben oltre la difesa del contenuto dei dati raccolti nei sistemi informatici; infatti estende il riconoscimento dello *jus excludendi alios* in capo a chiunque sia il titolare dei dati (persona fisica, giuridica, privata, pubblica) indipendentemente dal contenuto racchiuso negli stessi, purché si tratti di dati attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente, con la conseguenza che la tutela della legge si estende anche agli aspetti economici e patrimoniali dei dati. Il concetto di domicilio, inteso non più come un'area fisica dai confini materiali ben visibili e tangibili, bensì come un'espansione ideale dell'area di rispetto relativa a un soggetto, costituita e delimitata da informazioni: la norma, infatti, disciplina il reato di accesso abusivo ad un sistema informatico o telematico, punendo con la reclusione fino a tre anni chiunque abusivamente si introdu-

---

[(137)] Quinta Sezione Penale della Corte di Cassazione: Sentenza n. 47096 dell'11 dicembre 2007: *Delitti contro la persona – violazione di corrispondenza informatica - utilizzazione della password - conseguenze.* (Rif: *http://www.cortedicassazione.it/Documenti/47096sen_07.htm*)

ca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Con questa sentenza viene estesa la tutela del domicilio informatico, in quanto si riconosce il diritto di essere tutelato a chiunque abbia racchiuso nel proprio domicilio dei dati, indipendentemente dalla loro natura e da quella del titolare. In questo caso, la querela per accesso abusivo al sistema informatico può essere legittimamente proposta. Al fine di risolvere tale questione la legge 547/93 ha assicurato il riconoscimento giuridico di questo nuovo concetto di domicilio informatico, inteso come il bene giuridico per la cui tutela l'ordinamento garantisce il diritto di esplicare liberamente qualsiasi attività lecita all'interno del luogo informatico (inteso come spazio ideale, i cui confini "virtuali" sono rappresentati da informazioni), con facoltà di escludere terzi non graditi. Nel caso di specie, inoltre, sostiene la Corte, sono stati accertati tutti i requisiti previsti dall'art. 615-ter c.p. al fine della corretta configurazione del reato di accesso abusivo al sistema informatico.

Tale sentenza, seppur riguardando nello specifico un'azienda privata, risulta di grande interesse anche per le pubbliche amministrazioni, che devono anch'esse mettere in opera degli accorgimenti tecnici ed organizzativi necessari ad evitare intrusioni non autorizzate ai propri server di posta elettronica**,** a tutela del domicilio informatico dell'utente, anche in considerazione del fatto che l'accesso abusivo al sistema informatico è uno dei reati presupposto del D.Lgs. n. 231/2001 (in materia di responsabilità amministrativa).

5. Le tecnologie informatiche nei rapporti tra cittadini e P.A.

Si procederà ora ad analizzare quali siano i diritti, oltre all'attribuzione gratuita di un domicilio digitale, previsti dal Codice dell'Amministrazione Digitale e quali siano gli elementi che influiscono sulla possibilità e sulla volontà di esercitare tali diritti digitali per i cittadini. La consuetudine nell'effettuare comunicazioni e trasmissione di documenti da parte della pubblica amministrazione al domicilio digitale del cittadino comporterebbe notevoli vantaggi in termini di riduzione di spesa e di tempo impiegato nell'espletamento dei procedimenti; in alcuni casi la P.A. potrebbe trarre ulteriori guadagni, in tal senso si riporterà un esempio di come la certezza giuridica della notificazione via e-mail certificata di un provvedimento possa consentire la riduzione dei ricorsi accolti per decorrenza dei termini di notificazione.

5.1 I diritti all'uso delle tecnologie

Il legislatore negli ultimi quindici anni, partendo dalla L. 59/1997 (c.d. *Bassanini I*), in cui si affermava la validità giuridica dei documenti prodotti, trasmessi e archiviati con strumenti informatici, ha avviato un processo di ammodernamento finalizzato a rendere la pubblica amministrazione più efficiente attraverso l'utilizzo di tecnologie dell'informazione e della comunicazione.

Si è trattato sostanzialmente di regolamentare nuove realtà, situazioni, problematiche ma anche di recepire le nuove opportunità derivanti dai cambiamenti che la rapida evoluzione delle tecnologie informatiche e della rete nelle comunicazioni, hanno comportato nella società. La necessità di cambiamento della pubblica amministrazione, attuando un generale processo di ammodernamento, è una questione particolarmente sentita non solo in Italia, ma in tutti i paesi che costituiscono l'Unione Europea, tant'è che proprio dalla stessa Unione Europea proviene una delle prime e più compiute definizioni di e-Government: "*il ricorso alle tecnologie dell'informazione e della comunicazione nelle amministrazioni pubbliche, coniugato a un cambiamento organizzativo e all'acquisizione di nuove competenze da parte del personale, con*

l'obbiettivo di migliorare i servizi al pubblico, rafforzare il processo democratico e sostenere le politiche pubbliche"[137].

L'ammodernamento deve avvenire attraverso una serie di azioni che interessano i rapporti interni ad ogni singola amministrazione, tra le diverse amministrazioni e tra le stesse e i cittadini e le imprese. Le azioni da intraprendere richiedono un cambiamento della struttura delle relazioni che le amministrazioni stesse gestiscono, tali da creare un mutamento di costumi giuridici e sociali[138]. L'e-Government viene concordemente ritenuto un modo economico per migliorare il servizio ai cittadini e alle imprese, favorire la partecipazione e promuovere un'amministrazione aperta e trasparente. Le tecnologie dell'informazione e della comunicazione possono ridurre i costi e permettere alle amministrazioni pubbliche, ai cittadini e alle imprese di risparmiare tempo. Inoltre possono contribuire ad attenuare le minacce connesse ai cambiamenti climatici e ai rischi naturali e di origine umana grazie alla condivisione di dati ambientali e di informazioni sull'ambiente. In tal senso i governi europei, nell'ambito della più generale strategia *Europe 2020*[139], si sono impegnati a garantire entro il 2015 l'ampia diffusione

---

[137] *Il ruolo dell'eGovernment per il futuro dell'Europa*, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni - 26 settembre 2003, EUR-Lex.
(Rif: *http://eur-lex.europa.eu/legal-content/IT/NOT/?uri=CELEX:52003DC0567*)

[138] Rif: M.DELLA TORRE, pag. 129 in *[52]*

[139] Con la strategia *Europe 2020*, l'Unione europea si è posta priorità chiave e obiettivi per rilanciare il sistema economico e promuovere una crescita "intelligente, sostenibile e solidale" basata su un maggiore coordinamento delle politiche nazionali ed europee. Tra il 2000 e il 2010 l'UE ha cercato di migliorare crescita e occupazione con la Strategia di Lisbona (programma di riforme economiche approvato a Lisbona dai Capi di Stato e di Governo dell'Unione europea nel 2000).

Europe 2020, che succede a Lisbona, individua tre priorità:
- crescita intelligente
- crescita sostenibile
- crescita inclusiva.

(Rif: *http://ec.europa.eu/europe2020/index_en.htm*)

La Commissione europea propone cinque obiettivi da raggiungere entro il 2020:
- il 75% delle persone di età compresa tra 20 e 64 anni deve avere un lavoro;
- il 3% del PIL dell'UE deve essere investito in ricerca e sviluppo;
- i traguardi "20-20-20" in materia di clima/energia devono essere raggiunti: riduzione delle emissioni di gas serra del 20% (o persino del 30%, se le condizioni lo permettono) rispetto al 1990; 20% del fabbisogno di energia ricavato da fonti rinnovabili; aumento del 20% dell'efficienza energetica;
- il tasso di abbandono scolastico deve essere inferiore al 10% e almeno il 40% dei giovani (30-34enni) deve essere laureato;
- 20 milioni di persone in meno devono essere a rischio di povertà. (Segue in [139bis])

di servizi di e-Government orientati all'utente, personalizzati e multipiattaforma[140].

L'A*genda Digitale Europea*, una delle sette iniziative faro della strategia *Europe 2020* si propone di sfruttare al meglio il potenziale offerto dall'I.C.T. per favorire l'innovazione, la crescita economica e il progresso. L'obiettivo principale dell'Agenda è ottenere vantaggi socio-economici sostenibili grazie a un mercato digitale unico basato su Internet veloce e superveloce e su applicazioni interoperabili con la certezza che la maggiore diffusione ed un uso più efficace delle tecnologie digitali, consentirà ai cittadini una migliore qualità della vita, assicurando, ad esempio, un migliore servizio sanitario, trasporti più sicuri ed efficienti, nuove possibilità di comunicazione e un accesso più agevole ai servizi pubblici e ai contenuti culturali[141].

Tuttavia i benefici che i cittadini potrebbero trarre dall'uso delle tecnologie digitali sono necessariamente vincolati a molti e diversi fattori tra i quali i più significativi sono certamente la possibilità di disporre di un accesso ad internet, di avere la disponibilità di canali di comunicazione tali da consentire la riservatezza e la sicurezza dei dati trasmessi, l'usabilità[142] e l'accessibilità[143] delle piattaforme applicative, l'applicazione

---

(139bis) Sette sono le iniziative faro per catalizzare i progressi relativi a ciascun tema prioritario:
- Unione dell'innovazione per migliorare le condizioni generali e l'accesso ai finanziamenti per la ricerca e l'innovazione;
- Youth on the move per migliorare l'efficienza dei sistemi di insegnamento e agevolare l'ingresso dei giovani nel mercato del lavoro;
- Agenda europea del digitale per accelerare la diffusione dell'internet ad alta velocità e sfruttare i vantaggi di un mercato unico del digitale per famiglie e imprese;
- Europa efficiente sotto il profilo delle risorse;
- Politica industriale per l'era della globalizzazione;
- Agenda per nuove competenze e nuovi posti di lavoro;
- Piattaforma europea contro la povertà per garantire coesione sociale e territoriale.

(Rif: *http://europa.eu/legislation_summaries/employment_and_social_policy/eu2020/em0028_it.htm*)

(140) *European eGovernment Action Plan 2011-2015- Harnessing ICT to promote smart, sustainable & innovative, Government,* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (Rif: *http://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015,* 15.12.2010)

(141) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19 maggio 2010, *"Un'agenda digitale europea"*
(Rif: *http://europa.eu/legislation_summaries/information_society/strategies/si0016_it.htm,* 25.06.2010)

(142) L'usabilità è definita dall'ISO (International Organization for Standardization), come l'efficacia, l'efficienza e la soddisfazione con le quali determinati utenti raggiungono determinati obiettivi in determinati contesti. In pratica definisce il grado di facilità e soddisfazione con cui si compie l'interazione tra l'uomo e uno strumento (es. interfaccia grafica, ecc.). Il termine non si riferisce a una caratteristica intrinseca dello strumento, quanto al processo di interazione tra classi di utenti, prodotto e finalità.
(Rif: *http://it.wikipedia.org/wiki/Usabilit%C3%A0*)

di standard tecnologico-informatici che consentano l'interoperabilità dei software e l'accesso alle basi informative (ovviamente opportunamente regolamentato) e da ultimo ma più importante, la capacità dei cittadini di interagire con queste tecnologie.

L'Agenda Digitale Europea ha individuato una strategia unitaria a livello europeo volta al superamento di tutte le difficoltà rilevate definendo alcune aree d'azione da attuarsi a cura di ciascun Stato membro.

Queste aree d'azione sono definiti i *"pilastri"* dell'Agenda Digitale:

- Mercato digitale unico
- Internet veloce e superveloce
- Interoperabilità e standard
- Fiducia e sicurezza informatica
- Ricerca e innovazione
- Alfabetizzazione informatica
- ICT per la società.

L'Italia, come ognuno degli altri paesi, è chiamata ad analizzare il contesto nazionale per elaborare una propria strategia di recepimento dell'Agenda digitale, individuando le priorità e le modalità di intervento.

Vero è che il legislatore italiano, in materia di utilizzo delle nuove tecnologie, ha spesso *precorso i tempi*, nel senso che ha legiferato seguendo un'ottica forse più di *promozione* che di pura normazione.

Se si pensa in particolare all'impianto contenutistico del Codice dell'Amministrazione Digitale, è evidente che l'accento è stato posto sulla capacità delle nuove tecnologie di porsi quale strumento privilegiato di dialogo con i cittadini per ottenere un positivo impatto sui processi di comunicazione e di interazione tra P.A. e privati, nonché sull'organizzazione e sugli strumenti della pubblica amministrazione digitale.

---

(143) L'accessibilità è la caratteristica di un dispositivo, di un servizio, di una risorsa o di un ambiente d'essere fruibile con facilità da una qualsiasi tipologia d'utente.
(Rif: *http://en.wikipedia.org/wiki/Accessibility*)

Si può certamente affermare che ha provveduto a rendere "*obbligatoria l'innovazione nella P.A.*"[144], offrendo ai cittadini non solo la possibilità, ma il diritto, di interfacciarsi con la pubblica amministrazione attraverso le comunicazioni elettroniche e stabilendo, al contempo, che tutte le amministrazioni debbano organizzarsi in modo da rendere sempre disponibili i propri servizi in modalità digitale. Il legislatore ha sostanzialmente promosso nuovi strumenti e ne ha fondato la validità giuridica nella volontà di avere una amministrazione efficiente ed efficace.

Il C.A.D., pur individuando nella pubblica amministrazione il destinatario privilegiato delle disposizioni, in quanto incaricata dall'art. 2 ad assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, contiene importanti norme che si rivolgono alla generalità dei soggetti (inclusi cittadini, professionisti e imprese) soprattutto per quanto riguarda l'utilizzo di alcuni strumenti come il documento informatico, la firma elettronica, la p.e.c., il domicilio digitale e altri ancora, idonei a semplificare i rapporti tra Pubbliche amministrazioni, cittadini e imprese[145].

Il legislatore ha infatti riservato alla definizione dei diritti dei cittadini e delle imprese, in relazione alla fruizione di strumenti tecnologici, informatici e comunicativi, la Sezione II del Capo I (artt. 3-11) del C.A.D..

L'art. 3 afferma che i cittadini e le imprese hanno diritto all'uso delle tecnologie nelle comunicazioni con la pubblica amministrazione[146] e con i gestori di pubblici servizi. Si tratta dell'istituzione di un diritto, che prosegue e *si amplia* nei successivi articoli della stessa Sezione del Codice, che non si limita a configurare una pretesa

---

[144] Cit: A.LISI – L. GIACOPUZZI, pag. 19 in *[49]*

[145] *Sintesi introduttiva al Codice dell'Amministrazione Digitale*, (Licenza Creative Commons CC BY-NC 3.0 IT), 29 Marzo 2013, Progetto Formez PA. (Rif: *http://egov.formez.it/content/sintesi-introduttiva-codice-dellamministrazione-digitale*)

[146] In merito a cosa debba intendersi per amministrazioni pubbliche indicate all'art. 3 del C.A.D. si riporta quanto previsto dall'art. 1, comma 2 del decreto legislativo 30 marzo 2001, n. 165:
"*Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale*".

passiva del cittadino, ovvero il ricevere comunicazioni, ma farsi parte attiva, ovvero viene sancito il diritto del soggetto a partecipare al circuito tecnologico delle informazioni, il diritto all'autodeterminazione tecnologica, ed ancora, il diritto di accesso telematico[147].

Il diritto all'assegnazione di una casella di posta elettronica certificata personale gratuita costituita dal domicilio digitale, dell'art. 3-bis, istituisce il diritto del cittadino di disporre di un *comodo*, e giuridicamente valido, canale di comunicazione preferenziale con la P.A..

Si sancisce inoltre, all'art. 4, il diritto alla partecipazione al procedimento amministrativo informatico e il diritto di accesso ai documenti amministrativi mediante l'uso delle tecnologie dell'informazione e della comunicazione.

All'art. 5 viene indicata la facoltà di effettuare pagamenti, a qualunque titolo dovuti, alle amministrazioni e ai gestori pubblici servizi, anche con l'uso delle tecnologie dell'informazione e della comunicazione; l'art. 6 abilita coloro, che hanno dichiarato il proprio indirizzo p.e.c. secondo le modalità previste, allo scambio di documenti con le P.A. e all'art. 6-bis troviamo l'istituzione dell'INI-PEC.

Nell'art. 7 del Codice, rubricato *"Qualità dei servizi resi e soddisfazione dell'utenza"*, il legislatore chiede alle pubbliche amministrazioni di riorganizzare e aggiornare i servizi resi attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione sulla base delle reali esigenze delle società, anche per mezzo di strumenti atti a raccogliere il grado di soddisfazione degli stessi.

---

(147) Sul tema cit. di M.PIETRANGELO in *[51]*:
"Nell'ordinamento interno un generale diritto all'uso delle tecnologie trova già riconoscimento nel primo comma dell'art. 1della legge n. 4 del 20043, per il quale: 'La Repubblica riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione e ai relativi servizi, ivi compresi quelli che si articolano attraverso gli strumenti informatici e telematici'. Poiché tale legge, nota come 'legge Stanca', riconosce e garantisce ai soggetti disabili in particolare il diritto di accedere agli strumenti informatici (cfr. art. 1, co. 2), sul più generale riconoscimento a qualunque persona di tale diritto si è quasi taciuto."

Gli ultimi due articoli della sezione qui analizzata, (artt. 10 e 11) trattano dei diritti riguardanti specificatamente l'attività di impresa: l'art. 10 dispone che lo Stato, nell'ambito di quanto previsto dal Sistema Pubblico di connettività[148] realizzi un sistema informatizzato per l'accesso allo Sportello Unico per le attività produttive[149], mentre l'art. 11 istituisce il Registro informatico degli adempimenti amministrativi per le imprese[150].

In merito agli artt. 8 e 9, ed in conclusione dell'analisi della Sezione dei diritti, si evidenzia come essi non abbiano contenuto precettivo né per i cittadini né per la pubblica amministrazione: sono sostanzialmente dichiarazioni di intenti tese a favorire un avvicinamento all'uso delle tecnologie informatiche. In particolare l'art. 8 esprime la volontà dello Stato di promuovere iniziative volte a favorire l'alfabetizzazione informatica dei cittadini, con particolare riguardo alle categorie a rischio di esclusione, anche al fine di sostenere l'utilizzo dei servizi telematici delle amministrazioni pubbliche e l'art. 9 afferma che le p.a. favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti civili e politici siano, questi, individuali o collettivi.

---

[148] Il Sistema pubblico di connettività (SPC), istituito dall'art.72 del C.A.D. è costituito da un insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna P.A..

[149] Lo Sportello Unico per le Attività Produttive (SUAP), di cui all'art. 38 comma 3 D.L. 112/2008 convertito con modificazioni dalla L. 133/2008, eroga servizi telematici per l'avvio dell'attività o per ogni altro adempimento previsto nel ciclo di vita delle imprese.
(Rif: *http://www.impresainungiorno.gov.it/sportelli-suap*)

[150] Con l'art. 16 della legge 229/2003 è stato istituito il "Registro informatico degli adempimenti amministrativi per le imprese". Il Registro è istituito presso il Ministero delle attività produttive e si avvale del sistema informativo delle Camere di Commercio. Attraverso esso le imprese possono avere informazioni sugli adempimenti amministrativi previsti per l'avvio e l'esercizio di una qualsiasi attività economica. La norma prevede il collegamento con le banche dati degli sportelli unici per le imprese comunali e la possibilità per gli enti locali di avvalersi delle informazioni contenute nel Registro. L'istituzione di tale registro è stata riconfermata nell'art. 11 del C.A.D..
(Rif: *http://www.tuttocamere.it/modules.php?name=Content&pa=showpage&pid=251*)

I *diritti digitali* del cittadino nei confronti della pubblica amministrazione non possono essere naturalmente esercitati se il cittadino non ha le conoscenze, le capacità e le competenze che l'esercizio di questi diritti richiede.

"L'alfabetizzazione informatica è innanzitutto un presupposto logico, ancora prima che giuridico affinché alcuni diritti dei cittadini, riconosciuti da norme di legge, siano esercitabili. Ovviamente questi diritti non possono essere effettivi se il cittadino non ha "capacità" informatiche. Sotto il profilo logico, la previsione normativa non sarebbe applicabile. Finirebbe anzi con il produrre effetti negativi, perché aumenterebbe il digital divide. Cioè la diseguaglianza sociale fra chi è in grado di essere cittadino digitale e chi non è in grado. L'alfabetizzazione digitale è un dovere dello Stato per rendere effettivi alcuni diritti dei cittadini riconosciuti da norme primarie. La nostra Costituzione richiama il diritto all'istruzione, che però oggi ha un significato diverso. Inclusivo del digitale" [(151)] .

[(151)] Rif: G.FINOCCHIARO in intervista di A.LONGO a G.FINOCCHIARO, G.IACONO in *[50]*

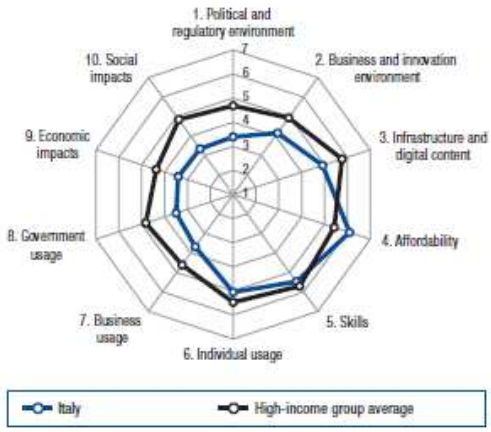
5.2 Il digital divide e la P.A.

Nell'ultimo rapporto del World Economic Forum[(152)], che rileva l'impatto dell'I.C.T. sullo sviluppo economico dei singoli Paesi, sui 144 paesi monitorati, si vede collocata l'Italia al 58° posto. Le maggiori criticità si rilevano nel basso impatto che le tecnologie dell'informazione e della comunicazione hanno sul sistema Paese e nel contesto generale economico e normativo. Il recente rapporto Eurostat[(153)], che riporta l'andamento dell'utilizzo di internet effettuato dalla popolazione dei 28 paesi dell'Unione Europea, rileva che il 62% degli individui tra i 16 e i 74 anni accedono ad Internet ogni giorno, o quasi ogni giorno, a fronte di un dato italiano del 54%. Il 79% delle famiglie europee ha un accesso ad internet fisso mentre in Italia la percentuale è pari al 69%. Il 21% dei cittadini europei ha dichiarato di non aver mai usato internet contro un 34% italiano. Infine, con specifico riferimento all'e-Government, in Europa

(152) Il rapporto del World Economic Forum mostra il Network Readiness Index, un indice con cui si esaminano i Paesi sulla base dell'impatto che l'I.C.T. ha sullo sviluppo economico di ogni Paese. Questo indicatore generale attribuisce una posizione sul combinato di 4 indici:
- contesto generale economico, normativo e infrastrutturale;
- grado di preparazione dei soggetti, individui, imprese e pubblica amministrazione nell'utilizzo;
- uso effettivo delle tecnologie;
- impatto delle I.C.T. sul sistema Paese.

Qui sotto è riportata la situazione italiana:

	Rank (out of 148)	Value (1–7)
Networked Readiness Index 2014	**58**	**4.2**
Networked Readiness Index 2013 (out of 144)	50	4.2
A. Environment subindex	**88**	**3.8**
1st pillar: Political and regulatory environment	99	3.4
2nd pillar: Business and innovation environment	76	4.1
B. Readiness subindex	**33**	**5.5**
3rd pillar: Infrastructure and digital content	42	4.9
4th pillar: Affordability	32	6.1
5th pillar: Skills	43	5.5
C. Usage subindex	**51**	**4.1**
6th pillar: Individual usage	37	5.0
7th pillar: Business usage	61	3.7
8th pillar: Government usage	112	3.5
D. Impact subindex	**82**	**3.4**
9th pillar: Economic impacts	58	3.4
10th pillar: Social impacts	94	3.3

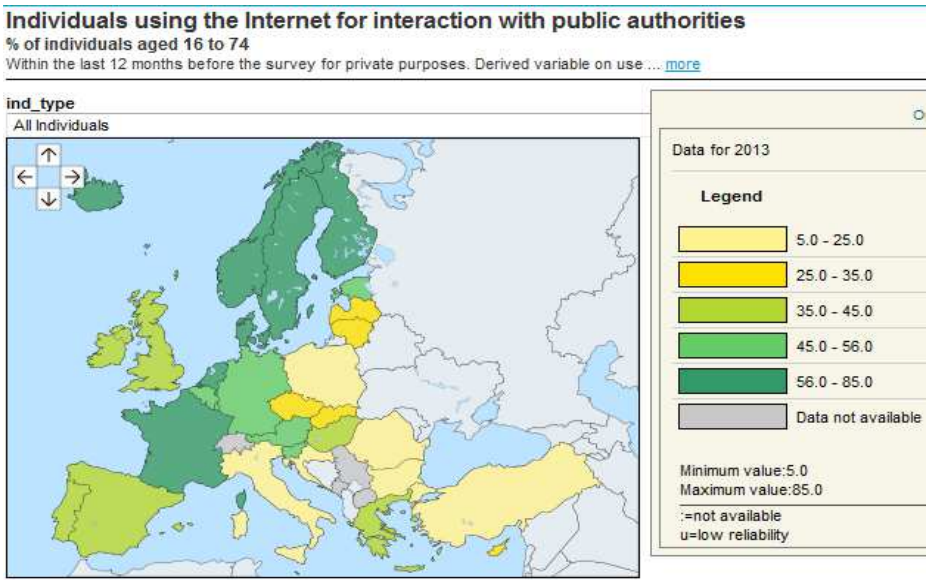


(The Global Information Technology Report 2014, The World Economic Forum, *http://reports.weforum.org/global-information-technology-report-2014/, pag. 163)*

La tredicesima edizione mostra che le prime sei posizioni restano immutate rispetto all'anno precedente: Finlandia, Singapore, Svezia, Olanda, Norvegia e Svizzera. Il nostro paese è al 58° posto, con una discesa rispetto all'anno precedente di otto posizioni.
(Rif: *http://www.weforum.org/issues/global-information-technology*)

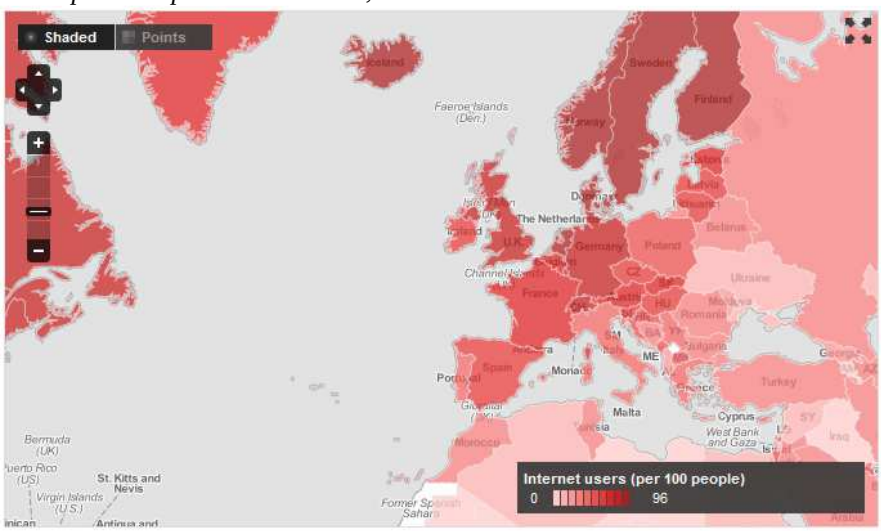
il 41% degli individui ha usato internet per interagire con la pubblica amministrazione principalmente per fini fiscali, richieste di documenti personali, sicurezza sociale e istruzione, mentre in Italia solo il 21% ha usufruito di servizi on-line per interagire con la pubblica amministrazione. In Italia, infine, ogni 100 persone, solo 58 possono disporre di un accesso ad internet sia esso fisso o mobile[154].

(153) *Internet access and use in 2013. More than 60% of individuals in the EU28 use the internet daily* Income tax declaration: most used e-government service, 18 December 2013, Eurostat Commission. STAT/13/199- 18/12/2013 *(*Rif: *http://europa.eu/rapid/press-release_STAT-13-199_en.htm)*



*(*Rif: *http://epp.eurostat.ec.europa.eu/tgm/mapToolClosed.do?tab=map&init=1&plugin=1& languag e=en&pcode=tin00079&toolbox=types#)*

(154) THE WORLD BANK - *Internet users (per 100 people) - Internet users are people with access to the worldwide network. International Telecommunication Union, World Telecommunication/ICT Development Report and database, and World Bank estimates*:

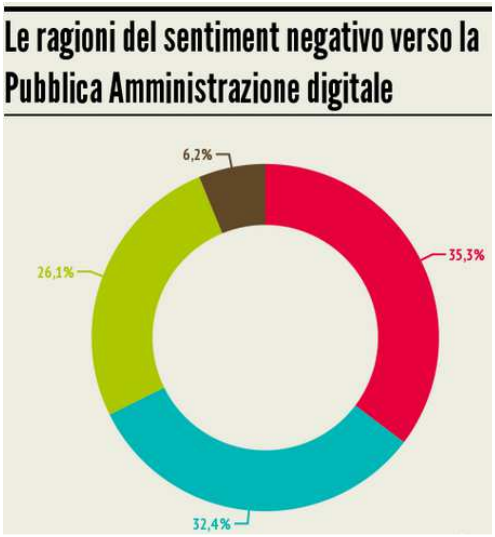


(Rif: *http://data.worldbank.org/indicator/IT.NET.USER.P2?order=wbapi_data_value_2012%20 wbapi_data_value%20wbapi_data_value-last&sort=as)c)*

Da una ricerca a cura di *Voices from the Blogs*[155] sulla percezione dei servizi della pubblica amministrazione negli ultimi tre mesi dello scorso anno, effettuata sui commenti reperiti sui più diffusi social network, emerge che, quando si parla dei servizi della pubblica amministrazione, i commenti complessivamente negativi sono pari al 38,8% del totale, mentre i pareri positivi si fermano al 26,6%. Quando si parla specificatamente dei servizi della P.A. digitale, i dissensi sono ancora maggiori: i commenti positivi rappresentano solamente il 22,5%, mentre i giudizi negativi arrivano al 47,9%.

Analizzando le cause del malcontento, i commenti più negativi (35,3%) fanno riferimento ai ritardi nel processo di introduzione delle nuove tecnologie e alle lentezze ritenute intollerabili da molti cittadini e imprese. Quasi un terzo di questi lamenta insufficienze delle infrastrutture dedicate, in primo luogo la scarsa diffusione della banda larga sul territorio nazionale. Una piccola parte (6,2%) lamenta l'assenza di un coordinamento centralizzato in grado di uniformare i servizi offerti e di farli dialogare tra loro in modo efficiente (ricorrente, ad esempio, la critica allo scarso livello di integrazione tra le banche dati degli enti della Pubblica Amministrazione). Ultimo dato particolarmente significativo, stante che questa rilevazione è stata effettuata su commenti di frequentatori della rete, è che nel 26,1% dei casi sono mostrate generali perplessità alla trasformazione dei servizi tradizionali in servizi digitalizzati e telematici e il timore diffuso è che la digitalizzazione dei servizi provochi una *"deprecabile spersonalizzazione"* del rapporto tra cittadino e burocrazia.

(155) *Pubblica Amministrazione digitale? La Rete ama ancora lo sportello!*, Voices from the Blogs (Osservatorio scientifico sui social media dell'Università Statale di Milano), 11 febbraio 2014.



La rilevazione del *Sentiment* cioè dell'atteggiamento emotivo nei confronti dei servizi informatici della P.A:

(Rif: *http://voicesfromtheblogs.com/2014/02/11/pa-digitale-no-grazie/*)

Gli obbiettivi definiti dall'Agenda Digitale Europea sono stati recepiti anche in Italia con l'istituzione dell'Agenda Digitale Italiana (ADI)[156] nel marzo 2012 con decreto del Ministro dello Sviluppo Economico, di concerto con il Ministro per la pubblica amministrazione e la semplificazione, il Ministro per la coesione territoriale, il Ministro dell'istruzione, dell'Università e della Ricerca e il Ministro dell'Economia e delle Finanze.

Con il D.L. 5/2012 (cd. *Semplifica Italia*) convertito in legge con modificazioni dalla Legge 35/2012 viene istituita una Cabina di Regia volta a definire una strategia nazionale per lo sviluppo del Paese puntando sull'economia digitale.

La Cabina di Regia ha individuato queste priorità:

- infrastrutture e sicurezza;
- e-commerce;
- e-government /open data;
- informatizzazione digitale e competenze digitali;
- ricerca e innovazione;
- smart communities.

Ciascuna di queste priorità deve concretizzarsi in specifiche linee di azione operative.

L'e-Government è ritenuto uno degli elementi cardine della modernizzazione previsto in *EUROPE 2020*. Gli obbiettivi fondamentali sono la creazione di una P.A. capace di operare in base a criteri di efficacia, efficienza, trasparenza, economicità e democrazia ed avviare un circolo virtuoso tra diffusione-utilizzo delle nuove tecnologie, qualità dei servizi pubblici, fiducia dei cittadini e partecipazione alla vita democratica che contribuisca all'emergere di un ambiente favorevole all'innovazione tecnologica, alla trasformazione e all'evoluzione dei modelli comportamentali e culturali ed alla crescita della competitività del Paese.

(156) Rif: *http://www.agenda-digitale.it/agenda_digitale/*

Le linee di azione in materia di e-Government italiane sono:

- Le “reti-Paese” e le infrastrutture logico-tecnologiche dell’e-Government che afferiscono alle tre grandi aree: affari interni, sanità e giustizia
- L’istituzione del domicilio digitale
- Sanità Digitale
- Giustizia e innovazione digitale
- Pubblica Amministrazione paperless
- Pubblica Amministrazione e fatturazione elettronica
- Moneta Elettronica
- Regole dell’amministrazione digitale
- Codice dell’amministrazione digitale
- Open Data.

In merito alle attività volte ad ampliare le competenze digitali, in quanto ritenute un fattore strategico di inclusione sociale, di alfabetizzazione, di innovazione, di cittadinanza attiva e di competitività del paese, si è ritenuto prioritario seguire queste linee d’azione:

- Estendere le azioni del Piano Nazionale “la scuola digitale”;
- Affrontare il problema dell’inclusione sociale;
- Incentivare il target femminile all’uso delle I.C.T.;
- Sensibilizzare all’uso critico e consapevole dei contenuti e dell’infrastruttura della rete;
- Promuovere l’uso delle I.C.T. nei vari settori professionali, del mondo del lavoro pubblico e privato, per garantire la riqualificazione e la formazione professionale continua;
- Promuovere la standardizzazione dei beni e dei servizi da acquistare, favorendo l’utilizzazione dell’e-procurement pubblico;
- Sostenere attraverso campagne di comunicazione istituzionale l’utilizzo delle tecnologie e la promozione delle conoscenze.

Le linee di intervento in materia di infrastrutture tecnologiche sono:

- Il Piano banda larga;
- Il Progetto strategico Banda Ultralarga;
- Il Progetto Data Center in modalità cloud computing.

Molte di queste linee si sono sviluppate in piani operativi già concretizzati, come in materia di giustizia, sanità, ecc., molte azioni sono attualmente in corso[157] e, sebbene avviate, non hanno ancora portato ad una diffusa percezione degli esiti sperati.

5.3 La P.A. e i vantaggi del domicilio digitale

Il digital divide, che investe anche la pubblica amministrazione, comporta ricadute negative a cascata sui cittadini. Da una P.A. digitale, e dalle persone che vi operano, sarebbe indispensabile attendersi, non solo l'abilità nell'uso delle tecnologie I.C.T., ma la capacità di modificare i processi lavorativi secondo nuove logiche che la tecnologia e la legge forniscono. Il legislatore, in merito all'alfabetizzazione informatica, all'art. 13 del C.A.D., attribuisce alle pubbliche amministrazioni il compito di curare la formazione del personale finalizzata alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione. La comprensione necessaria tuttavia non è solamente quella del mero utilizzo dello strumento informatico, ma ciò che occorre comprendere è come le tecnologie dell'informazione e della comunicazione possano modificare alla radice i processi organizzativi ed operativi della P.A. e questo richiede certamente un tempo fisiologico non certamente breve.

Altra questione è certamente legata alla connettività alla rete che, anche per le P.A., non sempre è garantita. Se non interverranno adeguamenti strutturali, il già presente rallentamento dei servizi e delle comunicazioni informatiche interne alle P.A. sarà destinato ad amplificarsi. Sono in fase di costituzione sistemi informativi integrati e banche dati centralizzate, come sarà l'ANPR, e ciò comporterà l'amplificazione del traffico di rete da parte delle pubbliche amministrazioni sia per interagire tra loro che per accedere a tali basi informative digitali.

[157] Sul sito dell'Agenzia per l'Italia Digitale è possibile consultare lo stato di avanzamento delle attività previste. *(*Rif: *http://www.agid.gov.it/)*

In questo contesto, occorre considerare ovviamente gli obbiettivi di e-Government che sono mirati ad aumentare l'interazione tra il cittadino e le amministrazioni non dimenticando che, ad oggi, non tutti i cittadini nel territorio nazionale possono connettersi ad internet e ciò comporta la loro automatica ed immediata esclusione da tutti gli strumenti e le procedure on-line che saranno predisposte dalle P.A..

Se la problematica non verrà risolta, potranno crearsi situazioni paradossali come nel caso di persone, residenti in aree a copertura di rete limitata, che dovranno continuare a recarsi fisicamente agli sportelli degli enti pubblici per richiedere un determinato servizio (che è disponibile on-line) e troveranno un impiegato allo sportello che dovrà farle attendere perché i *collegamenti sono lenti*.

Riportando il focus sulla casella di posta elettronica certificata assegnata al cittadino, certamente sussistono per le amministrazioni innumerevoli vantaggi. Il primo è sicuramente economico: le spese postali incidono notevolmente nei bilanci degli enti pubblici. Vero è che le comunicazioni via posta elettronica e via posta elettronica certificata tra pubbliche amministrazioni hanno notevolmente abbattuto i costi legati alla spedizione tradizionale ed è altrettanto vero che, in molte articolazioni dello Stato, la posta elettronica certificata non viene più necessariamente stampata ma integrata in sistemi di protocollazione documentale e fascicolazione elettronica. I medesimi vantaggi economici si ottengono dalle comunicazioni effettuate via p.e.c. anche con le imprese e i professionisti, stante la recente introduzione dell'INI-PEC. Il risparmio in termini economici e di tempo, che la pubblica amministrazione otterrebbe, inviando diffusamente le comunicazioni dalle proprie casella di posta certificata direttamente al domicilio digitale dei cittadini, sarebbe indubbiamente elevatissimo.

Per meglio spiegare quanto sino ad ora affermato, seppur non volendo entrare nella specificità della materia, si riporterà un esempio di cosa può accadere quando un organo dello Stato deve notificare al cittadino un verbale relativo ad un'infrazione al Codice della Strada (D.Lgs. n. 285/1992 e successive modificazioni ed integrazioni).

L'art. 201 comma 1 del Codice della Strada dispone "*Qualora la violazione non possa essere immediatamente contestata, il verbale, con gli estremi precisi e dettagliati della violazione e con la indicazione dei motivi che hanno reso impossibile la*

contestazione immediata, deve, entro novanta giorni dall'accertamento, essere notificato all'effettivo trasgressore…" ovvero l'organo accertatore ha dei limiti temporali, oltre che formali, entro cui procedere alla consegna del verbale al trasgressore (notifica).

I casi di contestazione non immediata da parte dell'organo accertatore sono piuttosto frequenti (eccesso di velocità, passaggio con semaforo rosso, rilevazione tramite telecamere di accesso non consentito, ecc.). La notificazione all'intestatario del veicolo viene effettuata dagli organi di Polizia, dai messi comunali o da un funzionario dell'amministrazione che ha accertato la violazione a mezzo del servizio postale. Le notificazioni si intendono validamente eseguite quando siano effettuate alla residenza, domicilio o sede, del soggetto risultante dalla carta di circolazione, dall'archivio nazionale dei veicoli istituito presso il Dipartimento per i Trasporti Terrestri o dal P.R.A. (Pubblico Registro Automobilistico).

Polizia di Stato, Carabinieri, Polizia Municipale, Guardia di Finanza, da anni utilizzano la posta elettronica certificata nelle comunicazioni con le altre pubbliche amministrazioni, ed in linea generale dispongono dei mezzi e del know-how necessari per notificare in maniera telematica una multa a un cittadino. Tuttavia, la notificazione per posta tradizionale è sostanzialmente l'unico canale utilizzato.

Uno dei problemi di molti organi dello Stato, ad oggi, è che non dispongono neppure di un accesso all'Anagrafe del Comune dove operano, tantomeno all'attuale Indice Nazionale delle Anagrafi. Accade così che uno degli ostacoli che si può frapporre tra il notificante ed il trasgressore è proprio la ricerca dell'indirizzo di quest'ultimo: per reperirlo, gli organi accertatori devono spesso effettuare ricerche in diverse banche dati. Le stesse possono non essere allineate con quelle dell'Anagrafe, di conseguenza spedire la raccomandata di notifica ad un vecchio indirizzo del trasgressore non è infrequente.

In seguito alla ricevuta di mancata consegna, il notificante dovrà procedere all'invio di un'altra raccomandata di notifica ad un nuovo indirizzo, reperito al termine di ulteriori interrogazioni informatiche, aumentando così i costi di spedizione ed i tempi di lavoro. Inoltre va ad amplificarsi il rischio di non riuscire in tempo utile ad effettuare la notifica ai sensi dell'art. 201 del Codice della Strada.

Una delle cause più frequenti di opposizione al Giudice di Pace, per ottenere l'annullamento di un verbale, è proprio l'errata notifica dello stesso[(158)].

La disponibilità del domicilio digitale del trasgressore consentirebbe al notificante di agire con la certezza di riuscire a reperire l'indirizzo del destinatario in tempo utile e con minori costi. Il trasgressore potrebbe opporsi solo fornendo la prova di essere stato, senza sua colpa, nell'impossibilità di aver avuto notizia del verbale (art. 1335 c.c.).

---

(158) La nullità della notifica può essere eccepita in diversi casi di cui qui si riportano alcuni esempi:

- laddove, in caso di notifica al portiere dello stabile, l'ufficiale giudiziario non certifichi di aver prima effettuato tutte le ricerche al fine di trovare il destinatario e/o i soggetti abilitati a ricevere l'atto ma si limiti a dare atto della precaria assenza del destinatario medesimo (Cassazione civile con sentenze 19417 del 11/9/2010 e n.2304 del 25/9/2007);
- laddove, in caso di notifica al portiere non venga prodotta raccomandata (ulteriore) con la quale l'ufficiale giudiziario comunica notizia al destinatario dell'avvenuto compimento delle formalità di cui all'art.139, comma 4 c.p.c. (Corte Costituzionale, sentenze n. 3/2010 e n. 258/2012; Cass. Sez. U., 627/2008; Ordinanza della Corte di Cassazione n.16050/11; Cass.Sez. U., 1418/2012);
- laddove, in caso di notifica ex art. 140 c.p.c., non possa ricavarsi l'avvenuto puntuale espletamento di tutte le prescritte formalità, e segnatamente il luogo di immissione dell'avviso (Cass. n. 13278/2013);
- laddove, in caso di notifica a mezzo del servizio postale ex art. 149 c.p.c., non venga prodotto l'avviso di ricevimento prescritto, poiché questo è il solo documento idoneo a provare sia l'intervenuta consegna, sia la data di essa, sia l'identità della persona a mani della quale è stata eseguita (Cfr. in tal senso, Cass. n. 26352/2011 e n. 13639/2010);
- laddove, in caso di notifica a persona diversa dal destinatario, non siano indicate le generalità del "consegnatario". La Cassazione con sentenza n. 14119/2013, ha infatti stabilito che "…dall'avviso di ricevimento deve risultare possibile l'identificazione della persona alla quale è stato consegnato l'atto e il principio così affermato è conforme con la giurisprudenza di questa Corte secondo la quale qualora manchi l'indicazione delle generalità del consegnatario, la notifica è nulla ai sensi dell'art. 160 c.p.c, per incertezza assoluta su detta persona, a meno che la persona del consegnatario sia sicuramente identificabile attraverso la menzione del suo rapporto con il destinatario" (Cfr. in tal senso, Cass. n. 12806/06; Cass. n. 4962/87; Cass. n. 1643/79; Cass. n. 4907/83);
- laddove, in caso di notifica a mezzo del servizio postale, la cartella sia priva della data di consegna indicata nella copia per il destinatario dell'atto. La Suprema Corte con la sentenza n. 398/12 specificava che "ai fini della validità della notifica ai sensi dell'art. 148 c.p.c., in caso di contrasto tra i dati risultanti dalla copia di relata allegata all'originale e i dati risultanti dalla copia consegnata al destinatario, occorre far riferimento alle risultanze ricavabili dalla copia in possesso del destinatario mentre, ove in questa manchi qualche elemento essenziale, la sua presenza nella relata allegata all'originale non è idonea ad escludere la nullità della notifica ai sensi dell'art. 160 c.p.c". Specificatamente, con riguardo alla mancanza, nella copia notificata consegnata al destinatario, della indicazione della data dell'eseguita notifica, è stato affermato che ciò comporta la nullità insanabile della notifica nel caso in cui da questa decorra un termine perentorio entro il quale il destinatario deve esercitare determinati diritti (Cfr. in tal senso, Cass. n. 14375 del 15 giugno 2010; Cass. n. 1210 del 19 gennaio 2007).

Le pubbliche amministrazioni, disponendo del domicilio digitale dei cittadini, potranno agire più celermente, sostenendo minori costi e contribuendo al raggiungimento degli obbiettivi di efficacia efficienza ed economicità previsti dall'Agenda Digitale italiana.

Conclusioni

L'attribuzione del domicilio digitale costituisce un diritto per il cittadino. Le amministrazioni pubbliche e i gestori o esercenti pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato.

Essendo il domicilio digitale una casella di posta elettronica certificata, si è indagato sulla diversa valenza giuridica di una e-mail e di una e-mail certificata, si è trattato il tema della tutela della privacy nelle comunicazioni via posta elettronica e dei reati penali previsti per le violazioni della corrispondenza informatica. Si è sperimentato l'utilizzo del servizio di Postacertificat@ e l'interoperabilità con le altre caselle di posta elettronica certificata.

All'attivazione dell'Anagrafe Nazionale della Popolazione Residente, prevista per il 31 dicembre 2014, il domicilio digitale sarà assegnato automaticamente al rilascio del documento unificato, oppure al momento dell'iscrizione anagrafica o alla dichiarazione del cambio di residenza e il cittadino avrà la facoltà di attivarlo successivamente. Al momento in cui si scrive tuttavia non stati emanati regolamenti attuativi per dettagliare le modalità di rilascio.

Il domicilio digitale è uno tra i tanti strumenti volti all'ammodernamento dell'azione dello Stato e consente di ottenere vantaggi consistenti in termini di riduzione di costi, tempi ed accelerazione generale delle comunicazioni. Per instaurare un positivo sistema di comunicazione digitale tra il cittadino e la p.a., questo strumento non dovrà certamente restare confinato all'utilizzo *punitivo*. Stante ad oggi l'attivazione volontaria, affinché il domicilio digitale trovi larga diffusione, dovrà essere percepito dal cittadino come un canale efficace per dialogare con la pubblica amministrazione e per ottenere celeri risposte. Per questa ragione sarebbe opportuno che le pubbliche amministrazioni promuovessero attivamente la fruizione di servizi che utilizzano come canale preferenziale il domicilio digitale.

Per concludere questo studio è doveroso affermare che sussistono alcuni significativi ostacoli di contesto che ne possono impedire il pieno utilizzo in tempi brevi. Primo tra tutti è certamente la scarsa alfabetizzazione informatica, che allontana immediatamente dai servizi digitali intere fasce sociali ed inoltre la non completata copertura di rete sul territorio nazionale lascia anch'essa cittadini impossibilitati ad accedere agevolmente ai servizi della P.A. digitale.

Se gli ostacoli di contesto verranno rimossi allora un numero maggiore di persone potrà esercitare il diritto all'utilizzo delle tecnologie informatiche nella comunicazione con la pubblica amministrazione e questo potrà incentivare la più ampia diffusione dei servizi della P.A. digitale, come il domicilio digitale del cittadino.

FONTI [*]:

[1] Francesco GALGANO, *Trattato di diritto civile*, Volume 1, Cedam, 2010.

[2] Andrea TORRENTE - Pietro SCHLESINGER, *Manuale di diritto privato*, Giuffrè, 2011.

[3] Saulle PANIZZA e Elettra STRADELLA, *Diritto pubblico*, Maggioli, 2013.

[4] Giovanni IUDICA e Paolo ZATTI, *Linguaggio e regole del diritto privato*, Cedam, 2003.

[5] Gianluca D'AIUTO e Luigi LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, 2012.

[6] Salvatore CACACE, *Codice dell'amministrazione digitale Dd.Lgs. n. 82/2005 e n. 159/2006. Finalità ed ambito di Applicazione – Diritti dei cittadini e delle imprese – Organizzazione delle pubbliche amministrazioni e tecnologie dell'informazione (http://www.giustizia-amministrativa.it/documentazione/Cacace_Codice_dell_amministrazione_digitale.htm)*

[7] Michele IASELLI, *Il testo unico della documentazione amministrativa ed il documento informatico*, Diritto&Diritti, 2001 (*http://www.diritto.it/articoli/tecnologie/iaselli2.html*)

[8] Giusella FINOCCHIARO, *Firma elettronica avanzata: oltre alle regole tecniche disposti anche obblighi di informazione e trasparenza*, Guida al Diritto 15.6.2013 - n. 25, pag. 16

[9] Giusella FINOCCHIARO, *Le copie per immagine su supporto informatico avranno l'efficacia probatoria degli atti originali – Decreto Legislativo 30 dicembre 2010 n. 235*, Guida al Diritto 19.2.2011 - n. 8, pag. 62

[10] Luigi FOGLIA e Francesca GIANNUZZI, *Le novità contenute nel nuovo CAD – Codice dell'Amministra-zione Digitale* – FORUM PA, 9.02.2011 (*http://saperi.forumpa.it/story/51323/le-novita-contenute-nel-nuovo-cad-codice-dellamministrazione-digitale)*

[11] Giusella FINOCCHIARO, *Scuola, sanità e notai comunicano su dati digitali*,Guida al Diritto 10.11.2012 - n. 45, p. 81

[12] Giusella FINOCCHIARO, *La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica*", Diritto dell'informazione e dell'informatica, 2013

[13] Andrea ROSSETTI, *Verba manent. Il documento digitale come atto sociale*, Relazione al convegno: La lumaca e la chiocciola. Collegio Ghislieri, 18 novembre 2010

[14] Manuela MILANESE, *L'atto pubblico informatico* (*http://www.comparazionedirittocivile.it/ prova/files/milanese_attopubblico.pdf*)

[15] Eugenio FAZIO, *Dalla forma alle forme. Struttura e funzione del neoformalismo negoziale*, pagg. 3-5, Università di Messina - Pubblicazioni della Facoltà di Giurisprudenza, 2011

[16] Giorgio DI BENEDETTO, *Scrittura privata e documento informatico. Riconoscimento, disconoscimento, verificazione*, ITINERARI NEL PROCESSO CIVILE, Giuffrè, 2009

[17] Massimiliano MINERVA, *Documento informatico e forma scritta*, 8 giugno 2005, FORUM 10 – Società dell'informazione, il futuro del diritto, i diritti del futuro, InterLex (*http://www.interlex.it/forum10/relazioni/30minerva.htm*)

[18] Filippo NOVARIO, *Le prove informatiche nel processo civile*, Giappichelli Editore, 2014

[19] Angelo FALZEA, Paolo GROSSI, Enzo CHELI, Umberto BRECCIA, *Enciclopedia del diritto. Annali, Volume 5*, Giuffre Editore, 2013

[20] Giusella FINOCCHIARO, *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, Contratto e impresa, n. 2, 2011.

[21] Andrea LISI, *Essere o non essere: i moderni dubbi amletici di una e-mail anonima*, Portale per l'Innovazione Digitale e l'Internazionalizzazione SCiNT, 18/02/2004 (*http://www.altalex.com/index.php?idnot=6915*)

[22] Laura TURINI, *Il valore probatorio del messaggio di posta elettronica*, Ventiquattrore Avvocato, ll sole 24 ore, 28.10.2004, pag 68.

[23] Beatrice SUCCI, *Ancora sull'email come prova*, Diritto&Internet, 30/12/2011 (*http://www.blogstudiolegalefinocchiaro.it/ documento-informatico-e-firma-digitale/ancora-sull%E2%80%99 email-come-prova/*)

[24] Giusella FINOCCHIARO, *Documento informatico - Ancora sull'efficacia probatoria del documento informatico non sottoscritto*, Diritto dell'Internet, n.6, 2005, p. 563

[25] Giuseppe CASSANO e Iacopo Pietro CIMINO ,*"Diritto dell'Internet e delle nuove tecnologie telematiche"*, Cedam, 2009

[26] Claudio PETRUCCI, Marco ORAZI, Francesco TORTORELLI, *La posta elettronica certificata*, Supplemento al n. 1/2007 del periodico Innovazione, CNIPA – Centro nazionale per l'informatica nella pubblica amministrazione

[27] Vincenzo GAMBETTA, *PEC – Posta elettronica certificata*, Collana di Minigrafie, Tecnologia dei Processi Documentali, Digit@LEX (*http://www.digita-lex.it/)*

[28] Fernanda FAINI, *E-government: le novità introdotte dal Decreto crescita 2.0*, Altalex, 25.01.2013 (*http://www.altalex.com/index.php?idnot=61233*)

[29] Riccardo BIANCHINI, *Aggiudicazione comunicata via Pec: quando scatta termine per impugnare?*, Altalex, 20.1.2014 (*http://www.altalex.com/index.php?idnot=66068*)

[30] Giusella FINOCCHIARO, *Per comunicazione e servizi più moderni ruolo di volano alla pubblica amministrazione – Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009*, Guida al Diritto 13.06.2009 - n. 24, pag. 26

[31] Gianni PENZO DORIA, *PEC e CEC-PAC: proviamo a fare chiarezza*, Altalex, 15.06.2010 (*http://www.altalex.com/index.php?idnot=11328*)

[32] Giorgio ZAPPA, *PEC, CEC PAC e firma elettronica: una guida all'utilizzo*, Risorse comuni - FIERAFORUM IX Edizione, Milano, atti del seminario del 24/11/2010 (*http://www.newscomuni.it/risorsecomuni2010/scheda_evento.asp?id_evento=880*)

[33] Governo italiano – Presidenza del Consiglio dei Ministri – Ministero per la semplificazione e la pubblica amministrazione, *Pec Day: nasce il servizio di posta elettronica certificata* (*http://www.funzionepubblica.gov.it/comunicazione/notizie/2010/aprile/26042010--pec-day-nasce-il-servizio-di-posta-elettronica-certificata.aspx*)

[34] Antonino MAZZEO - Intervista di Federica Meta, *La politica troppo distratta*, Corriere delle Comunicazioni n. 2 del 3/2/2014 (*http://www.corrierecomunicazioni.it/pa-digitale/25561_cec-pac-mazzeo-la-politica-troppo-distratta.htm*)

[35] Giorgio ROGNETTA, *La Comunicazione Elettronica Certificata (CEC-PAC): limiti e opportunità di utilizzo,* Altalex, 11.05.2010 (*http://www.altalex.com/index.php?idnot=10996*)

[36] Federica META, *Cec-Pac, cronaca di un flop,* Corriere delle Comunicazioni, inchiesta del 3/2/2014 (*http://www.corrierecomunicazioni.it/pa-digitale/25549_cec-pac-cronaca-di-un-flop.htm*)

[37] Luigi FOGLIA, *Domicilio digitale: il ritorno della CEC-PAC (e la fine del fax),* FORUM PA – Saperi PA, 19/09/2013 (*http://saperi.forumpa.it/story/73701/domicilio-digitale-il-ritorno-della-cec-pac-e-la-fine-del-fax*)

[38] Aldo MONEA, *Al debutto il domicilio digitale del cittadino*, Guida al Diritto 26.2.2013 - n. 1, p.70

[39] Telesio PERFETTI, *Il controllo della mailbox aziendale*, Diritto&Diritti, 07/12/2006, (*http://www.diritto.it/docs/23165-il-controllo-della-mailbox-aziendale*)

[40] Elena BASSOLI, *Come difendersi dalla violazione dei dati su internet. Diritti e responsabilità,* Maggioli Editore, 2013

[41] Ciro SANTORIELLO, Vito Sandro DESTITO, Giuseppe DEZZANI, Giuseppe AMATO, *I reati informatici: nuova disciplina e tecniche processuali di accertamento,* Cedam, 2010

[42] Piero TODOROVICH, *Privacy e marketing, le linee guida del Garante*, ITC4 Professional, 20/09/2013 (*http://www.ict4executive.it/professional/approfondimenti/privacy-e-marketing-le-linee-guida-del-garante_43672151979.htm*)

[43] Stefano AMORE, Vittorio STANCA, Sergio STARO, *I crimini informatici. Dottrina, giurisprudenziale ed aspetti tecnici delle investigazioni*, HALLEY, 2009

[44] Michele IASELLI, *Domicilio informatico: la Corte di Cassazione ne traccia i giusti confini*, Altalex, 7 dicembre 2012 (*http://www.altalex.com/index.php?idnot=59984*)

[45] Graziano GARRISI, *Il giudice protegge il domicilio informatico,* FORUM PA – Saperi PA, 23/01/2013 (*http://saperi.forumpa.it/story/69852/il-giudice-protegge-il-domicilio-informatico*)

[46] Emilio TOSI, *Contratti informatici, telematici e virtuali. Nuove forme e procedimenti formativi*, Giuffrè Editore, 2010

[47] Licia CALIFANO, *Il bilanciamento tra trasparenza e privacy nel d.lgs. 33/2013*, Assemblea Anci – Firenze, 24 ottobre 2013 (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2712616*)

[48] Roberto FLOR, V*erso una rivalutazione dell'art. 615 ter c.p.?*, Diritto penale contemporaneo n. 2/2012, pag. 126 (*http://www.penalecontemporaneo.it/*)

[49] Andrea LISI, Luca GIACOPUZZI, *Guida al codice dell'amministrazione digitale. Con focus su archiviazione e fatturazione elettronica*, HALLEY Editrice, 2006

[50] Alessandro LONGO – intervista a G.FINOCCHIARO, G.IACONO, *La lotta all'analfabetismo digitale*, 4 Maggio, 2014 Nòva, Il sole24ore (*http://nova.ilsole24ore.com/progetti/la-lotta-allanalfabetismo-digitale*)

[51] Marina PIETRANGELO, *Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione: luci ed ombre*, *Diritto* Amministrativo Elettronico 2005 – IV Convegno nazionale Catania, 1-2 luglio 2005 (*http://www.interlex.it/forum10/relazioni/44pietrangelo.pdf*)

[52] Massimiliano DELLA TORRE, *Diritto e informatica*, Giuffrè, 2009

[53] Ernesto BELISARIO, *La "nuova" pubblica amministrazione digitale,* Maggioli Editore, 2009

[54] Claudia MORGOGLIONE, *E.mail, liste, newsgroup non possono essere violati - Il principio vale anche per gli account aziendali ma solo "fino a prova contraria"*, 12 luglio 1999, Repubblica.it (*http://www.repubblica.it/online/internet/lettere/lettere/lettere.html*)

SITI INTERNET DI CONSULTAZIONE GENERALE:

- *http://www.normattiva.it/*
- *http://www.agid.gov.it/*
- *http://www.garanteprivacy.it*
- *http://www.diritto24.ilsole24ore.com*
- *http://www.agendadigitale.eu/*
- *http://www.corrierecomunicazioni.it/*
- *http://www.cortedicassazione.it*
- *http://www.funzionepubblica.gov.it/*

(*) L'esistenza di tutti i riferimenti alle pagine web presenti in questo scritto sono verificati al 30/6/2014.