Contributi di Dottrina

E-government e tutela dei dati personali: un quadro d'insieme

Emanuela Brugiotti*

Con il termine *e-government* si intende comunemente il processo di informatizzazione (1) della pubblica amministrazione, attraverso il quale è possibile trattare la documentazione e gestire i documenti stessi tramite strumenti digitali, grazie alle strutture proprie dell'ICT (2), allo scopo di rendere più snella ed efficiente l'attività degli enti locali e dell'amministrazione pubblica in generale, offrendo più servizi ai cittadini ed alle imprese, in un'ottica di trasparenza e fruibilità delle informazioni (3).

Negli ultimi anni il rapporto fra tecnologia e pubblica amministrazione ha visto il passaggio dall'introduzione dei primi strumenti informatici alla teleamministrazione e digitalizzazione delle attività amministrative.

In particolare, le politiche di *e-government*, contenute nei recenti interventi legislativi e regolamentari, hanno mirato non solo alla realizzazione di un sistema informativo volto all'automazione delle procedure interne della pubblica amministrazione e all'erogazione dei diversi servizi ai cittadini ed alle imprese, ma anche all'interconnessione fra i singoli sistemi informatici

(*) Avvocato in Roma, Dottore di ricerca in Giustizia costituzionale e diritti fondamentali nell'Università di Pisa, già praticante forense presso l'Avvocatura dello Stato.

(1) Ovvero il processo attraverso il quale il mezzo informatico rende un oggetto materiale (es. documento), interoperabile e consultabile attraverso il computer.

(2) ICT è l'acronimo di *Information and Communication Technology*, con questo termine si intende, generalmente, la possibilità di trasmissione dati attraverso apparecchiature informatiche, anche se nell'ultimo periodo il termine è pure usato per indicare gran parte del mondo informatico.

(3) Cfr. S. Stizia, *Informazione, nuove tecnologie e cambiamenti relazionali tra PA e cittadini*, in *Diritto dell'Internet*, Ipsoa, n. 6/2006, p. 615.

delle amministrazioni (4).

Fra le diverse implicazioni della digitalizzazione della p.a. si evidenzia in particolare, per l'argomento trattato in questa sede, l'aumento esponenziale della raccolta di informazioni, nonché la notevole riduzione delle distanze, anche in termini temporali fra produzione, elaborazione e diffusione delle stesse. Perciò questo pone la necessità di contemperare tale sviluppo con le esigenze di tutela della riservatezza, della protezione dei dati personali e della sicurezza informatica in generale (5).

Da questo punto di vista, quindi, l'*e-government* si intreccia necessariamente con la normativa in materia di *privacy* soprattutto quando viene richiesto alle pubbliche amministrazioni di rendere più fruibili ed accessibili i propri servizi, anche tramite strumenti che consentano al cittadino un'elevata autonomia ed interattività, come i siti *web* o la posta elettronica.

Volendo tracciare un quadro normativo ed istituzionale del fenomeno, si può dire innanzitutto che le azioni italiane in materia di sviluppo dell'*e-government* (o amministrazione digitale) sono per la maggior parte attuazione a livello nazionale di indirizzi stabiliti in sede comunitaria, ciò ad ulteriore conferma che oggi quasi tutte le questioni assumono ormai una dimensione transfrontaliera e globale (6).

Queste linee guida sono state efficacemente sintetizzate (7) in questi termini:

• creazione di un unico spazio europeo dell'informazione;

• innovazione e investimento nella ricerca;

• sviluppo e diffusione di servizi di amministrazione digitale per migliorare l'efficienza e l'efficacia della pubblica amministrazione;

• inclusione digitale, ovvero non lasciare indietro nessun cittadino rispetto alla fruizione di servizi di amministrazione digitale.

In Italia il recepimento di queste indicazioni si è mosso principalmente attraverso due direttrici: la definizione di un quadro normativo ed una serie di

---

(4) F. G. Angelini, *Pubblica amministrazione digitale, diritto di accesso e privacy*, in L. Bolognini, D. Fulco, P. Paganini (a cura di), *Next Privacy*, pag. 260. Per poter realizzare un sistema informativo integrato ed unificato è necessario garantire che due o più applicazioni residenti in più sistemi, abbiano la possibilità di interoperare tra loro. Così C. Silvestro, *E-government, e-governance, edemocracy*, in G. Cassano (a cura di), *Diritto delle nuove tecnologie informatiche e dell'Internet*, IPSOA 2002, pag. 1279-1281.

(5) Cfr. *E-government: il punto dei Garanti europei, Newsletter del Garante per la protezione dei dati personali n. 174 del 9-15 giugno 2003*, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=188992.

(6) Il Consiglio europeo con la Strategia di Lisbona, ratificata nel marzo del 2000, ha fissato, infatti, l'obiettivo "di fare dell'Unione Europea la più competitiva e dinamica economia della conoscenza del mondo" entro il 2010, sono seguiti poi i piani eEurope 2002, eEurope 2005 e la strategia i2010, vedi http://europa.eu/legislation_summaries/information_society/c11328_it.htm.

(7) F. S. Profiti, *Lo stato di attuazione dell'E-Goverment in Italia*, consultabile su http://www.cattolici-liberali.com/tocquevilleacton/pubblicazioni/focus/focus-paper20_ottobre08.pdf.

investimenti sia a livello di pubblica amministrazione centrale sia a livello regionale e degli enti locali, con la predisposizione di progetti cofinanziati.

Il nucleo dell'impianto normativo è costituito dal Codice dell'amministrazione digitale (CAD), emanato per la prima volta con D.lgs. 7 marzo 2005, n. 82 (8).

Il 19 febbraio 2010 il Consiglio dei Ministri, in virtù della delega contenuta nell'art. 33 della L. n. 69/2009, ha approvato il nuovo Codice dell'amministrazione digitale (9). La tecnica utilizzata è stata quella della novella legislativa. Infatti, il conseguente D.lgs. n. 235 del 30 dicembre 2010 (10) non ha sostituito il vecchio testo con uno nuovo, ma vi ha apportato direttamente le modifiche, operando sui vecchi articoli.

Le principali novità hanno riguardato: la riorganizzazione delle pubbliche amministrazioni (attraverso l'istituzione di un ufficio unico responsabile delle attività Ict (11)), la razionalizzazione organizzativa e informatica dei procedimenti, l'introduzione del protocollo informatico e del fascicolo elettronico, la semplificazione dei rapporti con i cittadini e con le imprese (attraverso l'introduzione di forme di pagamenti informatici, lo scambio di dati tra imprese e Pa, la diffusione e l'uso della Pec - Posta elettronica certificata), l'accesso ai servizi in rete, l'utilizzo della firma digitale - la dematerializzazione dei documenti e l'arricchimento dei contenuti dei siti istituzionali in termini di trasparenza.

Inoltre, è stata implementata la sicurezza dei dati attraverso la predisposizione, in caso di eventi disastrosi, di piani di emergenza per garantire la continuità operativa nella fornitura di servizi e lo scambio di dati tra Pa e cittadini.

Ancora, una volta operativo il nuovo CAD, il cittadino comunicherà una volta sola i propri dati alla PA centrale; sarà, poi, onere delle amministrazioni in possesso di tali dati assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre amministrazioni richiedenti.

In generale, comunque, sia il vecchio quanto il nuovo Codice, si inseriscono in un tessuto normativo volto alla costruzione di una nuova figura di pubblica amministrazione, maggiormente orientata verso i cittadini e *user friendly* (12).

---

(8) Consultabile su http://www.interlex.it/testi/dlg05_82.htm.

(9) Consultabile su http://www.innovazionepa.gov.it/media/350095/nuovo_codice_della_a mministrazione_digitale_cad.pdf; http://www.digitpa.gov.it/amministrazione_digitale.

(10) G.U. 10 gennaio 2011, n. 6, consultabile su http://www.gazzettaufficiale.it/guridb/dispatcher ?service=1&datagu=2011-010&task=dettaglio&numgu=6&redaz=011G0002&tmstp=1294735143548. Cfr. anche P. Ridolfi (a cura di), *Il nuovo Codice della Amministrazione Digitale, Collana di Minigrafie, Tecnologia dei Processi Documentali,* 2011, Fondazione Siav Academy - Edizione fuori commercio, consultabile sul sito http://www.digita-lex.it/pages/documents/ita/minigrafia7.pdf.

(11) Cfr. art. 17 Cad. A tale ufficio afferiscono i compiti relativi, tra gli altri, alla cooperazione e revisione della riorganizzazione dell'amministrazione, ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese, mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni, per la realizzazione e compartecipazione dei sistemi informativi cooperativi.

(12) E. Bassoli, *E-Government e privacy*, consultabile in www.federalismi.it.

Su questa linea, quindi, l'art. 3 commi 1, 1-*bis* e 1-*ter* del CAD ha previsto il diritto del cittadino e delle imprese all'uso delle tecnologie informatiche come strumento per l'interazione con la Pubblica Amministrazione.

La normativa ha disciplinato poi gli strumenti utilizzati normalmente per operare con la pubblica amministrazione e necessari nell'ambito dell'amministrazione digitale: la firma elettronica, in sostituzione della firma autografa, la posta elettronica certificata, in sostituzione della comunicazione via fax o via raccomandata a/r, regole per i pagamenti elettronici, lo sportello unico per le attività produttive anche in modalità telematica.

Infine, è stata promossa l'alfabetizzazione informatica dei cittadini, la formazione informatica dei dipendenti pubblici, lo scambio di informazioni tra pubbliche amministrazioni, attraverso modalità prettamente informatiche, basate sulle regole della Rete internazionale della pubblica amministrazione e del Sistema Pubblico di Connettività (SPC) (13).

Quest'ultimo, in particolare, è inteso come "l'insieme delle infrastrutture tecnologiche e delle regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione" necessarie per la realizzazione della "interoperabilità" - vale a dire dei servizi idonei a favorire lo scambio di dati e informazioni all'interno delle pubbliche amministrazioni e tra queste ed i cittadini - e della c.d. "cooperazione applicativa" che consente l'interazione tra i sistemi informatici delle pubbliche amministrazioni, permettendo così l'integrazione delle informazioni e dei procedimenti amministrativi (14).

Il Codice dell'amministrazione digitale, infatti, ha previsto l'accessibilità, da parte delle pubbliche amministrazioni, ai dati detenuti da altre amministrazioni secondo quello spirito di "leale cooperazione istituzionale" tra soggetti pubblici, già esplicitato nell'art. 22, comma 5, L. 241/90, definito ora, appunto, "cooperazione applicativa".

A tal fine, l'art. 14, comma 3 del CAD ha stabilito che lo Stato provveda alla creazione di organismi di cooperazione con le Regioni e le autonomie locali, promuovendo intese ed accordi tematici e territoriali, favorendo la collabora-

---

(13) F.S. Profiti, *Lo stato di attuazione dell'E-Goverment in Italia*, *op. cit.* Il Sistema Pubblico di Connettività (SPC) è stato istituito con il Decreto Legislativo 28 febbraio 2005, n. 42 (pubblicato nella Gazzetta Ufficiale n. 73 del 30 marzo 2005), successivamente confluito nel CAD. Al sistema pubblico di connettività il d.lgs. 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale, in G.U. n. 99 del 29 aprile 2006 – S.O. n. 105, ha dedicato l'intero Capo VIII "Sistema pubblico di connettività e rete internazionale della pubblica amministrazione".

(14) E. Bassoli, *E-Government e privacy*, *op. cit.*, pag. 11. In merito cfr. art. 68 Cad il quale appunto prevede che le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottino soluzioni informatiche che assicurino l'interoperabilità e la cooperazione applicativa e che consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano peculiari ed eccezionali esigenze.

zione interregionale, incentivando la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, così ad auspicare programmaticamente l'eliminazione del *digital divide* (15), tra amministrazioni di diversa dimensione e collocazione territoriale.

Anche per quanto concerne gli investimenti, di particolare rilievo è la forte collaborazione tra centro, regioni ed enti locali. Gli interventi sono stati articolati in due fasi distinte di attuazione (dette eGov fase I e eGov fase II).

Peraltro, il Sistema pubblico di connettività, previsto come indicato dal CAD, deve anche garantire "la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione" (16).

I diversi progetti previsti del Codice sono stati, fino a poco tempo fa, coordinati e monitorati dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (17) (CNIPA), attualmente, in seguito all'entrata in vigore del D.lgs. n. 177/2009 (il 29 dicembre 2009), questo ha assunto il nome di DigitPA (18), con il relativo trasferimento delle funzioni.

Il DigitPA è un ente pubblico non economico che opera secondo le direttive e sotto la vigilanza del Ministro per la Pubblica Amministrazione e l'Innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale.

L'ente svolge funzioni di natura progettuale, tecnica, operativa e di coordinamento nei confronti della pubblica amministrazione centrale e di quelle locali (19).

Si tenga presente poi che a gennaio del 2009 è stato presentato dal Ministero per la Pubblica Amministrazione e l'Innovazione un piano d'azione denominato "Piano *E-Government* 2012" (20), finalizzato a colmare il divario nell'applicazione delle tecnologie nei servizi pubblici da parte dei cittadini italiani rispetto a quelli europei, attraverso l'applicazione del Codice dell'amministrazione digitale e avendo come punto di riferimento il piano d'azione europeo sull'*e-goverment.*

Inoltre, con la legge finanziaria del 2006 è stata istituita l'Agenzia per la diffusione delle tecnologie per l'innovazione (21), con lo scopo di integrare il

---

(15) *Digital divide*, è il termine tecnico utilizzato per definire le disuguaglianze nell'accesso e nell'utilizzo delle tecnologie.

(16) Art. 73 comma 2 del CAD.

(17) http://www.cnipa.gov.it/.

(18) http://www.digitpa.gov.it/.

(19) Cfr. http://www.digitpa.gov.it/digitpa/funzioni.

(20) http://www.e2012.gov.it/egov2012/index.php.

(21) L'Agenzia per la diffusione delle tecnologie per l'innovazione, istituita con la legge finanziaria 2006, opera a livello nazionale ed è sottoposta ai poteri di indirizzo e vigilanza del Ministero per la Pubblica Amministrazione e l'Innovazione. Ha la finalità di accrescere la capacità competitiva delle piccole e medie imprese e dei distretti industriali attraverso la diffusione di nuove tecnologie e delle re-

sistema della ricerca con quello produttivo attraverso l'individuazione, valorizzazione e diffusione di nuove conoscenze, tecnologie, brevetti ed applicazioni industriali prodotti su scala nazionale ed internazionale.

Fra gli elementi di maggior rilievo nella struttura dell'*e-government* deve essere segnalato il cd. "fascicolo informatico" (22), strumento cardine dell'intero *iter* procedimentale (23).

Secondo quanto disciplinato dal Codice, le regole per la costituzione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico (24) ed il sistema pubblico di connettività. In ogni caso queste devono rispettare i criteri dell'interoperabilità e della cooperazione applicativa.

Inoltre, il fascicolo è consultabile e integrabile da parte di tutte le amministrazioni che intervengono nel procedimento (25), pur essendo nella sua costituzione e gestione curato dall'amministrazione titolare del procedimento.

Il fascicolo informatico, inoltre, deve avere i requisiti della facile reperibilità, corretta collocazione e collegabilità; in più è costituito e gestito in modo da consentire l'esercizio in via telematica dei diritti di cui alla L. n. 241 del 1990.

Quanto è stato brevemente illustrato mette in evidenza come questo generale processo di automazione e integrazione tecnologica nella p.a., sia nella sua organizzazione sia nei suoi rapporti con i soggetti privati, pone inevitabilmente anche problematiche legate alla necessità di tutela del diritto alla *privacy*, in considerazione della enorme quantità di dati che entrerà, come osservato, nel patrimonio informativo delle diverse pubbliche amministrazioni, anche per il pregresso.

Non sono mancate al riguardo iniziative dell'Autorità garante, la quale

---

lative applicazioni industriali e di promuovere l'integrazione fra il sistema della ricerca e il sistema produttivo attraverso l'individuazione, la valorizzazione e la diffusione di nuove conoscenze, brevetti ed applicazioni industriali prodotti su scala nazionale e internazionale. http://www.aginnovazione.gov.it/it/index.html.

(22) Art. 41 del Codice dell'amministrazione digitale.

(23) Relazione illustrativa al decreto legislativo 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale, in G.U. n. 99 del 29 aprile 2006, S.O. n. 105.

(24) Con il D.P.R. 428/98 - in seguito abrogato dal D.P.R. 445/2000 - il legislatore ha emanato il regolamento per la gestione del protocollo informatico che viene definito come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dalle amministrazioni per la gestione dei documenti". Con questo atto vengono fissati per la prima volta a livello normativo, i criteri generali. Sull'argomento cfr. E. Bassoli, *E-Government e privacy*, *op. cit*., pag. 17 e ss.; http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Protocollo_informatico/;http://www.interlex.it/pa/prot_norme.htm; P. Ridolfi, *Amministrazione digitale. Compendio normativo*, *Collana Minigrafie, Tecnologia dei processi documentali,* Fondazione Siav Academy, 2010, consultabile sul sito www.digita-lex.it.

(25) L'art. 41 del Codice prevede, quindi, una gestione flessibile del fascicolo da parte della pubblica amministrazione titolare, tuttavia il fascicolo può contenere aree riservate, cui hanno accesso solo la medesima P.A. o alcuni soggetti da essa individuati.

ha segnalato diverse volte la necessità di una maggiore precisione e proporzionalità nell'identificazione della tipologia dei dati da inserire nei documenti, le persone che vi possono accedere e le garanzie da apprestare, soprattutto in relazione ai dati sanitari e biometrici.

Senza contare che comportamenti illeciti ed inidonee misure di sicurezza, oltre a ledere diritti, ostacolano la diffusione e l'uso delle tecnologie all'interno del tessuto economico e sociale, alimentando la diffidenza nei confronti delle stesse (26).

Il Codice dell'amministrazione digitale ha posto regole di garanzia in materia di tutela dei dati personali sia a livello generale sia in riferimento a singoli istituti. Dal primo punto di vista, l'art. 2 comma 5 ha sancito che le disposizioni del Codice "si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato".

All'interno della normativa, invece, ad esempio in tema di firme elettroniche e certificatori (27), l'art. 27 comma 2 lett. e) ha previsto, poi, che il soggetto certificatore adotti "adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi" (28).

Così come è stato previsto il rispetto della normativa a tutela dei dati personali per quanto riguarda, in generale, il trattamento e la disponibilità dei dati da parte delle pubbliche amministrazioni, la sicurezza e l'accesso agli stessi (29).

---

(26) Cfr. ad esempio quanto riportato su http://ansa.it/site/notizie/awnplus/internet/news/2009-05-12_112376716.html o http://www.helpconsumatori.it/news.php?id=23353.

(27) Ai sensi dell'art. 1 lett. g) del CAD il certificatore è "il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime".

(28) Di seguito l'art. 32, comma 5, ha prescritto che "il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono".
Ancora, in tema di segretezza della corrispondenza trasmessa per via telematica, l'art. 49 comma 1, ha imposto che "gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche".

(29) Cfr art. 50. Disponibilità dei dati delle pubbliche amministrazioni e art. 52. Accesso telematico e riutilizzazione dei dati e documenti delle pubbliche amministrazioni.

Bisogna sottolineare, al riguardo, che anche in quest'ambito un ruolo fondamentale è svolto proprio dalla sicurezza e, in questo settore in particolare, dalla sicurezza del sistema informatico della pubblica amministrazione (30).

Infatti, "qualunque informazione una Pubblica Amministrazione maneggi che sia riconducibile a cittadini identificati o identificabili - quindi pressoché tutte - deve essere protetta", così "quando noi parliamo di Pubbliche Amministrazioni in senso lato accade che la sicurezza sia oggi l'oggetto principale della *privacy* ", perché "la *privacy* è la sicurezza, la sicurezza è la tutela dei dati dei cittadini" (31).

A tal fine, ai sensi dell'art. 71 comma 1 *bis* del Codice dell'amministrazione digitale è stato emanato il DPCM (1 aprile 2008) (32), contenente le regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività.

Il Decreto ha previsto che le funzioni di referente centrale nazionale per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza nel SPC siano svolte dal *Computer Emergency Response Team* del Sistema Pubblico di Connettività (CERT-SPC) (33), sul modello adottato a livello internazionale. La struttura, già operativa dall'inizio del 2008 all'interno del CNIPA (ora DigiPA), ha finito per sostituire il precedente GovCert (34).

Le suddette Regole tecniche hanno disposto, poi, che ogni amministrazione centrale aderente all'SPC si doti di una Unità Locale di Sicurezza (ULS), cui è affidata sia la responsabilità di porre in atto tutte le fasi di prevenzione degli incidenti ICT, sia la gestione operativa degli eventuali incidenti informatici.

Fra gli strumenti dell'*e-government* maggiormente posti all'attenzione

---

(30) Cfr. art. 51 CAD.

(31) Così F. Pizzetti, *Sicurezza, privacy, efficienza dei servizi: come conciliare i diritti per lo sviluppo di una moderna pubblica amministrazione*, Roma, 22 novembre 2007, consultabile su http://www.forumpa.it/convegni/sicurezzaprivacy/documenti/Pizzetti.pdf. Si vedano anche *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*, del 19 marzo 2011, Gazzetta Ufficiale n. 64 del 19 marzo 2011, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1793203. Ancora, *Linee guida per la sicurezza Ict nelle pubbliche amministrazioni*, http://www.cnipa.gov.it/site/_files/Quaderno%20n%2023.pdf; http://www.cert_spc.it/ index.php/download/govcert /1469-normativa-e-linee-guida.

(32) Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-*bis* del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»" G.U. 21 giugno 2008, n. 144. Consultabile su http://www.cnipa.gov.it/HTML/RN_ICT_cron/spc_DPCM%201%20aprile%202008.pdf.

(33) http://www.cert-spc.it. Per le Regioni, le Regole Tecniche stabilisco la presenza di un CERT-SPC-R. A tal fine è operativo un gruppo di lavoro con le Regioni per definire, attraverso intese, le modalità di partecipazione al sistema di sicurezza SPC, si veda ad esempio il Protocollo d'Intesa tra il CNIPA e la Regione Toscana, consultabile su http://www.e.toscana.it/e-toscana/resources/cms/documents/PI_cnipa_rt_8Lug2008.pdf .

(34) http://www2.cnipa.gov.it/site/_contentfiles/01380100/1380130_SEMINARIO_SICUREZZA_CNIPA.pdf.

pubblica e che più coinvolgono la vita del singolo cittadino, devono a questo punto segnalarsi, in particolare, la posta elettronica certificata e le carte elettroniche. Per questo di seguito se ne illustrano gli elementi fondamentali.

Per quanto riguarda la Posta Elettronica Certificata (PEC) (35), questa consiste in un tipo speciale di *e-mai*l che consente di inviare/ricevere messaggi di testo e allegati, con lo stesso valore legale di una raccomandata con avviso di ricevimento, e rappresenta uno degli strumenti più importanti nel processo di digitalizzazione delle amministrazioni pubbliche.

La Pec, quindi, è fra le priorità del Piano di *e-Government* 2012, in cui è inserita come progetto "Casella elettronica certificata" (36).

Il CAD ha prescritto che le amministrazioni utilizzino la PEC per comunicare con i soggetti che hanno dichiarato il loro indirizzo, ai sensi della vigente normativa tecnica (art. 6), e sono dotati di una casella PEC per ciascun registro di protocollo (art. 47, c. 3). Inoltre, ha stabilito che le comunicazioni di documenti tra le PA sono valide, ai fini della verifica della provenienza, se trasmesse attraverso sistemi di PEC (art. 47, c. 2).

In base all'art. 48 del CAD, la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante PEC o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA. Tale trasmissione equivale alla notificazione per mezzo della posta, salvo che la legge disponga diversamente.

Norme più recenti poi hanno esteso la portata della PEC, come strumento di scambio di documenti, dal solo ambito delle amministrazioni a quelli delle imprese, dei professionisti e dei cittadini (37).

Per quanto riguarda in particolare la tutela dei dati personali, specifica

---

(35) D.P.R. n. 68/2005, consultabile su http://archivio.cnipa.gov.it/site/_files/DPR%2011%20febbraio%202005%20n.68.pdf. Ai sensi dell'art. 1 comma 1 v-*bis* del Codice dell'amminsitrazione digitale, per posta elettronica certificata si intende il "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"; cfr. http://www.digitpa.gov.it/sites/default/files/digitpa_minig_11_alta_0.pdf; https://www.postacertificata.gov.it /guida_utente/normativa-di-riferimento.dot e P. Ridolfi, *Amministrazione digitale. Compendio Normativo*, *op. cit*., pag. 78 e ss.; cfr. ancora V. Gambetta, *Pec, Posta Elettronica Certificata*, *Collana di Minigrafie*, 2011, Fondazione Siav Academy.

(36) Da aprile 2010 tutti i cittadini italiani - anche se residenti all'estero - hanno diritto gratuitamente a una casella di posta elettronica certificata (PEC) per effettuare via internet, con le pubbliche amministrazioni, comunicazioni di cui sia necessario certificare la spedizione, in sostituzione della raccomandata con ricevuta di ritorno. Cfr. http://www.digitpa.gov.it/pec/pec-al-cittadino; http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Posta_Elettronica_ Certificata__%28PEC%29/.

(37) La PEC per il cittadino (tecnicamente designata come CEC-PAC) può essere utilizzata solo per le comunicazioni con le Pubbliche Amministrazioni. Per comunicare con altri indirizzi PEC è necessario acquistare una casella PEC commerciale. Riguardo alle caselle della pubblica amministrazione, la comunicazione è limitata alle pubbliche amministrazioni iscritte all'Indice P.A.(IPA). Cfr. http://www.digitpa.gov.it/pec/pec-al-cittadino e per la relativa normativa cfr. http://www.digitpa.gov.it/pec/ normativa.

importanza svolge la sicurezza del servizio di trasmissione telematica di messaggi e documenti (38). Oltre a quanto precedentemente osservato relativamente alla sicurezza del sistema pubblico di connettività, qui si evidenzia che tutte le connessioni sono realizzate tramite l'impiego di canali sicuri, basati sull'utilizzo dei protocolli di trasporto *Transport Layer Security* (TLS)/*Secure Sockets Layer* (SSL), che permettono la crittografia dei dati trasmessi in rete, mentre, per quanto riguarda i virus, vengono effettuati controlli sia nei messaggi in ingresso che in uscita.

Le configurazioni adottate, inoltre, sono tali per cui tutti i messaggi di PEC in cui è rilevata la presenza di virus sono consegnati al motore di Posta-Certificat@ per essere trattati in conformità alla normativa vigente.

Ancora, le registrazioni (*log*), inerenti i messaggi scambiati, sono memorizzati su un registro riportante i dati significativi dell'operazione. I *log* dei messaggi sono conservati per 30 mesi a cura del gestore (39).

Infine, per quanto riguarda la posta elettronica certificata, il Digitpa svolge sia un ruolo di vigilanza sui gestori del servizio sia di supporto alle pubbliche amministrazioni per la sua introduzione nei procedimenti amministrativi (40).

Quanto alle garanzie per il trattamento dei dati personali da parte delle pubbliche amministrazioni, oltre a quelle già indicate (41) previste dal CAD, l'art. 46 dello stesso Codice ha prescritto in particolare che "al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite".

---

(38) Si vedano il Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (G.U. 15 novembre 2005, n. 266), consultabile su http://www.digitpa.gov.it/sites/default/files/normativa/DM_2-nov-2005.pdf e l'Allegato al Decreto 2 novembre 2005 "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata", il quale contiene tutte le regole e le specifiche tecniche per l'utilizzo della PEC, consultabile su http://www.digitpa.gov.it/sites/default/files/normativa/Pec_regole_tecniche_DM_2-nov-2005.pdf.

(39) Per quanto riguarda l'Indice P.A. (IPA), vedi http://www.indicepa.gov.it/, mentre per la sicurezza vedi https://www.postacertificata.gov.it/guida_utente/sicurezza.dot. Esempi di fattori critici per il trattamento dei dati personali possono rinvenirsi nel fatto che la conservazione per 30 mesi delle ricevute include anche l'intero messaggio e suoi eventuali allegati, anche se il gestore PEC è l'unico ad avere le credenziali per aprire "la busta di trasporto", non possono essere esclusi tentativi di accesso da parte di terzi dovuti a vulnerabilità del servizio del gestore o accessi abusivi di soggetti dello stesso. Il gestore dovrà, quindi, munirsi di adeguate misure di sicurezza. Un altro nodo delicato relativo al trattamento dei dati personali è che la normativa non stabilisce dove vada a finire tutta la corrispondenza PEC e le informazioni in essa contenute dopo i trenta mesi.

(40) http://www.digitpa.gov.it/pec/ruolo-digitpa.

(41) Vedi ad es. l'art. 49 del CAD, cit., che ha assoggettato alla segretezza il contenuto della corrispondenza trasmessa per via telematica. Ed in generale gli artt. 50 e ss. del CAD, cit.

Infine, l'art. 47 comma 3 del CAD, ha previsto che l'utilizzo della posta elettronica per le comunicazioni fra l'amministrazione ed i propri dipendenti avvenga mediante la posta elettronica o altri strumenti informatici di comunicazione, "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".

Passando ora alle carte elettroniche - ovvero la Carta di Identità Elettronica (CIE), la Carta Nazionale dei Servizi (CNS) ed il passaporto elettronico - questi sono strumenti, come detto, ritenuti essenziali per l'ammodernamento della pubblica amministrazione e sono individuati nelle politiche di *e-government*, fra l'altro, come mezzi attraverso i quali gli utenti vengono riconosciuti in rete in modo certo, al fine di usufruire dei servizi erogati per via telematica dalle amministrazioni pubbliche (42).

In particolare, la carta d'identità elettronica (CIE) (43) è uno strumento di identificazione personale nonché di autenticazione per l'accesso ai servizi *web* erogati dalle Pubbliche Amministrazioni, come previsto dal Codice dell'amministrazione digitale (art. 66). Le regole tecniche del nuovo documento di riconoscimento personale sono state indicate nel Decreto Interministeriale dell'8 novembre 2007 (44).

La carta contiene tutti i dati identificativi e le informazioni ufficiali relative alla persona e funzionerà anche come carta di servizi (45).

Oltre ai dati identificativi personali, ai sensi dell'art. 66, comma 4 del Codice dell'amministrazione digitale, la carta d'identità elettronica può contenere,

---

(42) Cfr. P. Corsini, E. Orbini Michelacci, *Sostituire il documento cartaceo con il documento informatico, firmarlo e trasmetterlo in rete*, in "Diritto dell'Internet", Ipsoa, n. 3/2006, p. 311; P. Ridolfi, *Amministrazione digitale. Compendio normativo*, cit., pag. 63 e ss.

(43) La carta d'identità elettronica è una *smart card* che integra nel supporto in policarbonato una banda ottica e un microprocessore. Più specificamente, i dati del titolare, compresa la foto, sono impressi in modo visibile sia sul supporto fisico, per l'identificazione "a vista", che sulla banda ottica e poi memorizzati informaticamente sul microchip e ancora sulla banda ottica. Per la normativa di riferimento cfr. http://www.cnipa.gov.it/site/it-it/Normativa/Raccolta_normativa_ICT/Carta_d%E2%80%99identit%C3%A0_elettronica_e_carta_nazionale_dei_servizi/. Ai sensi dell'art. 1, comma 1 lett. c) del Cad, per carta d'identità elettronica si intende "il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare".

(44) G.U. 9 novembre 2007 n. 229, S.O. n. 261, consultabile su http://www.cnipa.gov.it/HTML/RN_ICT_cron/08/agg05/ ci_20071108_DM.pdf.

(45) La Carta Nazionale dei Servizi è una *smart card* provvista esclusivamente del microchip (su un supporto fisico che non è necessariamente in policarbonato). Contrariamente alla CIE non si tratta in questo caso di un documento per l'identificazione a vista ma di uno strumento di autenticazione in rete che consente l'accesso ai servizi della P.A. resi disponibili per via telematica. La CNS è regolamentata ai sensi del decreto del Presidente della Repubblica 2 marzo 2004, n. 117 (G.U. 6 maggio 2004, n. 105) che ne stabilisce le modalità d'uso e di diffusione. La completa corrispondenza informatica tra CNS e CIE assicurerà l'interoperabilità tra le due carte e la continuità di servizi all'utente che passi dalla Carta Nazionale dei Servizi alla Carta d'Identità Elettronica. Cfr. E. Bassoli, *E-Government e privacy*, *op. cit*., pag. 20.

"a richiesta dell'interessato, ove si tratti di dati sensibili: a. l'indicazione del gruppo sanguigno; b. le opzioni di carattere sanitario previste dalla legge; c. i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA; d. tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza; e. le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica".

L'introduzione all'interno della carta d'identità elettronica, per fini di semplificazione amministrativa, di altri dati diversi da quelli anagrafici e non strettamente necessari per la funzione di identificazione personale, ha posto, già al suo affacciarsi nel panorama legislativo, diverse questioni in ordine alla tutela della riservatezza dei cittadini.

La quantità di dati, anche sensibili, raccolta su ogni cittadino rischia di diventare in vero e proprio archivio, il cui utilizzo illegittimo potrebbe creare non pochi problemi. Già in riferimento alla Carta dei Servizi, il Garante espresse la necessità di particolari cautele e regole che evitassero la formazione di banche dati omnicomprensive, così come la raccolta e l'uso di dati personali in violazione dei principi di necessità, pertinenza e finalità (46).

Al riguardo, l'art. 8 del DPCM 22 ottobre 1999, n. 437 (47) ha stabilito che sono dettate con decreto del Ministero dell'interno (48) le regole tecniche e di sicurezza, relative alle tecnologie ed ai materiali utilizzati per la produ-

---

(46) Si veda il parere del Garante al Ministero per l'innovazione tecnologica del 2003, di cui un sunto è contenuto nella newsletter del Garante n. 177 del 7 - 13 luglio 2003, consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID =246147; quanto osservato da G. Buttarelli nel 2002 al Convegno: "Carta di identità elettronica e firma digitale: dalla sperimentazione ai servizi": " << Si tratta di dati, questi ultimi - ha precisato il Segretario generale - che in realtà aprono una serie di questioni riguardanti da un lato la loro effettiva utilità nell'essere inseriti nella carta di identità elettronica e la loro successiva utilità da parte di terzi, siano essi enti pubblici o strutture private e, dall'altro, gli aspetti tecnici su come effettivamente raccoglierli ed inserirli >>. Altri aspetti delicati derivano dal modo con cui sono registrati e accessibili, dalle tecnologie e dalle finalità prescelte (…) << L'Autorità garante - ha proseguito Buttarelli - ha perciò il compito istituzionale di richiamare l'attenzione nelle sedi istituzionali nazionali e negli organismi internazionali competenti sulla questione, in modo tale che la carta di identità elettronica possa garantire adeguate certezze riguardo alla protezione dei dati personali >>", cfr. http://www.garanteprivacy.it/garante/doc.jsp?ID=45900; ancora, G. Rasi nell'ambito del Convegno: "La sicurezza partecipata: coordinamento e cooperazione interistituzionale" svoltosi all'interno nell'ambito del Forum P.A. 2004: " <<La preoccupazione istituzionale dell'Autorità Garante per la protezione dei dati personali si è focalizzata sulla necessità che i nuovi strumenti tecnologici, finalizzati ad una fluidificazione dei rapporti tra cittadini e Pubblica amministrazione, non confliggano con il rispetto della persona e con le garanzie di riservatezza e sicurezza dei dati personali>> (…) In particolare, adeguata attenzione dovrà essere posta nella definizione delle regole tecniche e delle misure di sicurezza che dovranno essere garantite al cittadino affinché in caso, ad esempio, di smarrimento o furto, la Carta possa essere immediatamente "invalidata" a garanzia dei dati in essa contenuti", cfr. http://www.garanteprivacy.it/garante/doc.jsp?ID=1001758.

(47) G.U. n. 277 del 25 novembre 1999. Consultabile su www.privacy.it/dpcm19991022.html.

(48) Cfr. D.M. 8 novembre 2007, cit., consultabile anche su www.interno.it.

zione delle carte d'identità elettroniche, alle modalità di compilazione, rilascio, aggiornamento e rinnovo dei documenti e per garantire l'integrità, l'accessibilità e la riservatezza delle informazioni contenute nel documento.

Lo stesso articolo 8 ha previsto, poi, che le suddette regole tecniche e di sicurezza devono essere adeguate all'evoluzione delle conoscenze scientifiche e tecnologiche con cadenza almeno biennale.

Altra questione, legata all'inserimento di ulteriori dati all'interno delle carte d'identità elettroniche e del loro futuro uso come carte dei servizi delle pubbliche amministrazioni, è quella del cd. codice d'identificazione unico.

In molti paesi esiste già un identificatore unico utilizzato dai cittadini per i contatti con la pubblica amministrazione. Può trattarsi di un identificatore settoriale, come il codice fiscale italiano, oppure di un numero unico nazionale, come accade in Svezia e Finlandia (49).

Un altro strumento di rilievo dell'*e-government* è il passaporto elettronico che dal 26 ottobre 2006 viene rilasciato dalle questure ed dagli uffici consolari italiani all'estero. Il documento, realizzato con particolari metodi di stampa anti contraffazione, è dotato di un microchip e di un microprocessore che consente la registrazione dei dati e certificati, riguardanti il titolare dello stesso e dell'Autorità che lo ha rilasciato.

Inoltre, dal 19 maggio 2010, data dell'entrata in vigore del decreto 303/13 del 23 marzo 2010 (50), viene emesso il "nuovo passaporto ordinario".

Ai sensi dell'art. 2 del suddetto decreto, "nel chip sono, memorizzate, in formato interoperativo, l'immagine del volto e le impronte digitali del titolare.

---

(49) Per un'interessante panoramica dei documenti d'identificazione in diversi paesi europei ed extraeuropei, nonostante la traduzione italiana non perfetta, cfr. http://www.worldlingo.com /ma/enwiki/it/National_identification_number/1. Si evidenzia, inoltre, che il 25 ottobre 2010, hanno preso il via sei progetti pilota, inseriti nel progetto generale denominato STORK, finanziato dal Programma europeo di Sostegno alle Politiche ICT (ICT-PSP) del Programma Quadro Competitività e Innovazione (CIP). Nell'ambito del progetto STORK è stata realizzata una piattaforma europea per l'interoperabilità delle identità elettroniche (eID) ed il 25 ottobre è stato appunto annunciato che i sei progetti piloti sono disponibili al pubblico: Autenticazione trans-frontaliera per servizi elettronici, Chat più sicura, Mobilità degli studenti, Trasmissioni elettroniche trans-frontaliere, Cambio di residenza e l'integrazione col portale dei servizi della Commissione Europea. Questa piattaforma consente ai cittadini di utilizzare il proprio identificativo elettronico nazionale in diversi Stati europei. I sei progetti piloti, avviati ufficialmente, saranno gradualmente migliorati e ne sarà verificata l'integrazione con i servizi dei portali attivi della piattaforma di interoperabilità di STORK. Cfr. http://www.digitpa.gov.it/notizie/avviati-i-sei-progetti-pilota-di-stork-l%E2%80%99interoperabilit%C3%A0-dell%E2%80%99identit%C3%A0-elettronica-tutta-eu.

(50) Consultabile su http://www.governo.it/GovernoInforma/Dossier/passaporto_ordinario /decreto_23_marzo_2010.pdf. Cfr. anche il Regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 28 maggio 2009, che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, GUUE L 142 del 6 giugno 2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:IT:NOT e http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:188:0127:0127:IT:PDF.

Nel chip sono altresì memorizzate le informazioni, già presenti sul supporto cartaceo, relative al passaporto ed al titolare, nonché i codici informatici per la protezione ed inalterabilità dei dati e le informazioni necessarie per renderne possibile la lettura agli organi di controllo.

Gli elementi biometrici contenuti nel chip potranno essere utilizzati solo al fine di verificare l'autenticità del documento e l'identità del titolare attraverso elementi comparativi direttamente disponibili quando la legge lo prevede. I dati biometrici raccolti ai fini del rilascio del passaporto non saranno conservati in banche di dati".

Particolari meccanismi di sicurezza sono finalizzati a garantire l'autenticità, la integrità e la riservatezza dei dati contenuti nel chip.

In particolare, sono previsti due tipi di controllo degli accessi alla lettura dei dati registrati nel chip: il primo, *Basic Access Control* (BAC) per evitare la lettura dei dati senza il permesso del titolare del documento, il secondo, *Extended Access Control*, (EAC) per consentire la lettura dei file contenenti le immagini delle impronte ai soli soggetti autorizzati dallo Stato emettitore.

La Nazione che rilascia passaporti biometrici contenenti impronte digitali può stabilire, per mezzo dell'EAC, i Paesi o i servizi che potranno leggere le impronte digitali registrate (51).

Queste misure toccano uno degli aspetti critici del passaporto elettronico che, utilizzato prevalentemente per spostarsi da un paese all'altro, espone i dati in esso contenuti ad una diffusione anche esterna. Perciò sono necessarie, appunto, particolari cautele.

Riguardo alla tutela dei dati personali contenuti nei passaporti, si segnala a livello internazionale, la "Risoluzione sull'utilizzo della biometria in passaporti, carte di identità e titoli di viaggio" del 2005, in occasione della 27ma Conferenza internazionale delle Autorità di protezione dei dati e della *privacy*, in cui quest'ultime hanno preso atto che "governi e organismi internazionali, ed in particolare l'Organizzazione internazionale dell'aviazione civile (ICAO), stanno attualmente completando la definizione di norme e *standard* tecnici volti ad integrare dati biometrici (impronte digitali, riconoscimento del volto) in passaporti e titoli di viaggio ai fini della lotta al terrorismo e della velocizzazione dei controlli alle frontiere e delle procedure di imbarco".

Pertanto, le stesse Autorità chiedono che "si limiti tecnicamente l'impiego della biometria in passaporti e carte di identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso" (52).

---

(51) *Tecnologie Biometriche per il controllo delle frontiere nell'Unione europea*, consultabile su http://www.cnipa.gov.it/;html/docs/BIOMETRIA%20E%20SICUREZZA%20DELLE%20FRONTIERE.pdf.

(52) Consultabile su http://www.garanteprivacy.it/garante/doc.jsp?ID=1170552.

Sempre in merito alla sicurezza dei dati raccolti in questi documenti d'identificazione, si segnalano a livello comunitario il Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (53), il parere del 30 settembre 2005 del Gruppo di lavoro dei garanti europei sull'attuazione del suddetto regolamento (54), le decisioni della Commissione europea C (2005) 409 del 28 febbraio 2005 e C (2006) 2909 del 28 giugno 2006, sulle caratteristiche di sicurezza rispettivamente degli elementi biometrici primari e secondari nei passaporti e nei documenti di viaggio ed, infine, il Regolamento del Consiglio dell'Unione europea n. 444/2009 del 6 maggio 2009 (55), il quale modifica il precedente Regolamento del 2004.

Anche in questo ambito, quindi, i principi cardine richiamati sono quelli di un elevato livello di sicurezza, della qualità dei dati (i dati personali devono essere adeguati, pertinenti, non eccedenti), della legittimità dei trattamenti e dell'adeguata informazione agli interessati.

(53) GUCE L 385 del 29 dicembre 2004, pagg. 1-6, consultabile su http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:IT:HTML.

(54) Consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_it.pdf.

(55) GUUE L 142 del 6 giugno 2009, consultabile su http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:32009R0444:IT:NOT, v. , anche la relativa Rettifica, GUUE L 188/127 del 18 luglio 2009, consultabile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:188:0127:0127:IT:PDF.