DISPENSE PROF. AVV. MARCO MANCARELLA

CORSO DI INFORMATICA GIURIDICA

CDL SCIENZE POLITICHE E DELLE RELAZIONI INTERNAZIONALI

CAPITOLO 1
EVOLUZIONE DEL C.A.D. E NOVITA' DELLA RIFORMA 2018

1.1. Evoluzione normativa delle norme sull'amministrazione digitale

La tappa fondamentale del processo di digitalizzazione della pubblica amministrazione, è senz'altro rappresentato dal Codice dell'amministrazione digitale (da ora C.A.D.), adottato in origine con D.Lgs. 7 marzo 2005, n. 82.

Esso rappresenta senza dubbio il principale atto legislativo in materia di sviluppo della pubblica amministrazione, ed in genere dei rapporti tra consociati, verso l'uso delle nuove tecnologie informatiche.

Ma non si tratta del primo provvedimento legislativo italiano in materia.

Con il C.A.D. il legislatore italiano ha inteso riunire e riordinare le norme già esistenti, integrandole con nuove disposizioni, proprio al fine di racchiudere in un'unica fonte i principi, le regole e gli istituti fondamentali per il raggiungimento dell'obiettivo della digitalizzazione e della dematerializzazione dell'attività amministrativa, in modo tale da porre le basi per una struttura burocratica più efficiente e rapida e, soprattutto, meno costosa.

Tra tali provvedimenti previgenti si segnalano, in particolare, la legge 15 marzo 1997 n. 59, cd. Legge Bassanini; il DPR 10 novembre 1997 n. 513, ovvero il regolamento attuativo su formazione, archiviazione e trasmissione di documenti con strumenti informatici, che per primo in Europa ha dettato una disciplina esaustiva di firma digitale e documento informatico; il DPR n. 445 del 28 dicembre 2000, recante testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa; la legge 9 gennaio 2004 n. 4, cd. Legge Stanca, sull'accessibilità degli strumenti informatici; il DPR 11 febbraio 2005 n. 68, che ha istituito un sistema di posta elettronica certificata, unico nel mondo, sempre discusso, ma ad oggi divenuto ormai esclusivo canale di comunicazione tra PA, imprese e professionisti.

Il testo del C.A.D., come anticipato, non si focalizza esclusivamente sull'operato della pubblica amministrazione; il legislatore ha infatti approfittato di tale provvedimento per introdurre da un lato una serie di strumenti e nozioni che esplicano la loro efficacia anche al di fuori dell'ambito amministrativo (si pensi alla posta elettronica certificata, alla firma digitale, alla generalizzazione

della rilevanza dei documenti informatici) e, dall'altro, per sancire una serie di diritti innovativi per cittadini e imprese (ad esempio, il diritto all'uso delle nuove tecnologie, l'accesso e il diritto alla trasmissione di documenti in formato digitale, il diritto ai pagamenti con modalità elettronica).

E proprio per la peculiarità della materia oggetto del provvedimento in parola, sempre esposta a rapidissimi mutamenti ed evoluzioni, si è reso più volte necessario intervenire sul testo originario, avvalendosi dello strumento del decreto correttivo previsto dalle varie leggi delega susseguitesi negli anni, per adeguare l'assetto legislativo alle nuove esigenze ed ai nuovi approdi.

Dopo il primo correttivo, emanato a stretto giro con il D.Lgs. 4 aprile 2006 n. 159, il secondo correttivo è intervenuto con il D.Lgs. 30 dicembre 2010 n. 235, modificando più di 50 articoli ed introducendo nuove disposizioni, tra le quali, in particolare, il <<fascicolo informatico obbligatorio>> per ogni pubblica amministrazione titolare del procedimento (art. 41, comma 2, C.A.D.),

Il terzo correttivo è stato licenziato con il D.lgs. 26 agosto 2016 n. 179, in forza della delega contenuta all'art. 1 della L. 7 agosto 2015 n. 124, rubricato enfaticamente <<Carta della cittadinanza digitale>>, la cui priorità era per l'appunto quella di promuovere ed assicurare il diritto dei cittadini e delle imprese di accesso ai dati ed ai servizi in modalità digitale. Tale riforma era peraltro quanto mai opportuna alla luce del c.d. Regolamento EIDAS, n. 910 del 2014, con cui l'Unione Europea aveva nel frattempo ridisegnato un quadro omogeneo a livello europeo sul tema della digitalizzazione, e che, non necessitando di alcun atto di recepimento, sarebbe comunque entrato in vigore in Italia il 1 luglio 2016.

I due punti cardine di questo terzo intervento sono la <<qualità del servizio>> e la <<partecipazione>> dei cittadini. Il cittadino, infatti vanta nei confronti dell'amministrazione il diritto ad un servizio pubblico qualitativamente alto, al quale può partecipare direttamente e del quale ha diritto a rimanere soddisfatto. È stato inoltre previsto che ciascun cittadino sia dotato di un domicilio digitale, da comunicare al comune di residenza, mediante il quale si potranno inviare e ricevere comunicazioni nei rapporti con la PA. Si rafforza, in tal modo, il ruolo della posta elettronica certificata quale mezzo ordinario di comunicazione, sicura ed affidabile, equiparata alla notificazione a mezzo posta ai sensi dell'art. 48 del C.A.D..

L'ultimo correttivo in ordine di tempo è il D.lgs. 13 dicembre 2017 n. 217, entrata in vigore il 27 gennaio 2018, che opera alcune rilevantissime modifiche.

Riguardo all'ambito di applicazione, si dispone per la prima volta l'applicazione del C.A.D. anche agli atti e agli avvisi di accertamento, di rettifica e liquidazione e di irrogazione delle sanzioni emessi dall'Agenzia delle entrate.

Novità importanti, che verranno approfondite nei capitoli successivi, riguardano anche il domicilio digitale e le firme elettroniche. Quanto al domicilio digitale ogni cittadino potrà eleggere un proprio domicilio digitale, anche a prescindere dall'operatività dell'Anagrafe della Popolazione Residente (ANPR), che finalmente costituirà l'unico recapito per ogni amministrazione pubblica italiana.
Per quanto riguarda le firme elettroniche, in particolare il correttivo 2018 ha previsto una nuova applicazione software equipollente alla firma digitale: <<il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi e' apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, **e' formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID** ai sensi dell'articolo 71 con modalita' tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore>> (art. 20 comma 1-bis, C.A.D.).

1.2. Le nuove fonti di normazione secondaria: le linee guida AgID

Sin dalle prime battute della relazione illustrativa del correttivo n. 217/2017, viene fuori l'intento del legislatore di deregolamentare l'attuazione del Codice dell'amministrazione digitale, nell'ottica di una maggiore semplificazione, sostituendo quelle che nelle precedenti versioni del C.A.D. erano le regole tecniche, adottate con Decreto del Presidente della Repubblica, con Linee Guida, la cui emanazione è di competenza dell'AgID.
La ratio giustificativa sottesa alla sostituzione delle regole tecniche con le linee guida è quella di <<rendere l'attuazione tecnico-operativa delle disposizioni di legge capace di stare al passo con la continua evoluzione tecnologica, scongiurando il rischio che le regole finiscano con l'imbrigliare amministrazione e cittadini a utilizzare soluzioni e servizi meno moderni di quelli disponibili sul mercato>> (Analisi d'Impatto Regolamentare al decreto correttivo del Codice dell'Amministrazione Digitale).
La deregolamentazione dell'attuazione del C.A.D. si allinea al trend che si è registrato negli ultimi anni in tema di aggiornamento legislativo e normativa attuativa, ed è un fenomeno a cui abbiamo già assistito con l'entrata in vigore del nuovo codice dei contratti pubblici. d.lgs. 18 aprile 2016 n. 50. Se prima la regolazione di attuazione era affidata alle fonti di rango secondario regolamentare, con il Codice degli appalti si è passati ad affidare il compito di attuare la legge alla c.d. soft law.
Il concetto di soft law non è proprio del nostro ordinamento ma è tipico del diritto anglosassone, in cui viene utilizzato per la regolamentazione di situazioni non direttamente disciplinate dalla c.d. hard law o legge vincolante di rango primario.

In Italia la soft law si è concretizzata nelle linee guida, che dai regolamenti differiscono, oltre che per la natura giuridica dell'atto, anche a prima vista, nell'impostazione e nel drafting, risultando più discorsive e analitiche.

Ma come si collocano le linee guida nel sistema della gerarchia delle fonti? Secondo alcuni le Linee Guida sono atti normativi particolari, emanati da un'autorità amministrativa, hanno una forma specifica e stabiliscono un particolare vincolo giuridico. Esse sono norme, ed hanno – come punti nodali del loro ciclo di vita – la determinazione, modificazione, abrogazione e specialmente l'interpretazione e l'applicazione (ITALIA). Altri invece riconducono le linee guida al genus degli atti amministrativi generali non normativi.

Al fine di individuare la collocazione delle linee guida all'interno del nostro ordinamento è utile capire la differenza tra atti normativi e atti amministrativi generali.

I primi sono atti emanati da organi cui la legge espressamente attribuisce il potere di emanare atti normativi e sono caratterizzati dalla generalità, intesa come la capacità di rivolgersi ad un numero indeterminato ed e indeterminabile di soggetti e dell'astrattezza, intesa come la capacità di regolare una pluralità indeterminata di casi.

L'emanazione di un atto normativo ha come effetto quello di regolare un ambito nuovo, ancora non regolato ovvero di abrogare la regolamentazione vigente, provocando delle modificazioni all'interno dell'ordinamento giuridico.

All'interno della gerarchia delle fonti, gli atti normativi si collocano secondo un ordine che vede in cima i precetti costituzionali, poi le leggi ordinarie e infine i regolamenti.

I regolamenti sono una fonte di rango secondario la cui emanazione rientra nella potestà normativa del governo, ed il cui procedimento di emanazione è disciplinato ai sensi dell'art. 17 della L. 400/1988. Essi vengono emanati in forma di Decreti del Presidente della Repubblica e Decreti Ministeriali, e la loro adozione è prevista attraverso un iter specifico che vede il coinvolgimento del Consiglio di Stato e delle Commissioni Parlamentari in veste consultiva.

Tali norme regolamentari hanno la capacità di regolare materie per le quali non sussiste una riserva assoluta di legge, e di abrogare altre fonti di rango secondario. Inoltre, le amministrazioni, nello svolgimento della loro attività e nell'emanazione dei loro atti, sono obbligati a osservare il precetto normativo, senza che alle stesse sia attribuito il potere di disattenderne il contenuto, dal momento che la violazione dei decreti comporta l'illegittimità del provvedimento emanato. Il loro carattere normativo altresì li rende atti non immediatamente lesivi e pertanto non direttamente impugnabili, se non unitamente ai provvedimenti che ad essi danno attuazione.

Gli atti amministrativi generali sono caratterizzati invece dalla generalità, intesa come la capacità di rivolgersi ad una pluralità indeterminata di soggetti, ma non dall'astrattezza, in quanto non sono atti applicabili ad una pluralità indeterminata di casi.

Proprio il venir meno del requisito dell'astrattezza li distingue, prima facie, dagli atti normativi. A tele differenza si aggiunge quella di non essere sottoposti ad un iter formativo vincolante, come quello della l. 400/88 che di questi ultimi determina la legittimità, nel rispetto del principio di legalità sostanziale. Inoltre, a differenza degli atti normativi, gli atti amministrativi generali possono produrre effetti immediatamente lesivi, unicamente in forza della loro emanazione, ed effetti non immediatamente lesivi che necessitano di un ulteriore provvedimento attuativo che determini tale lesione.

Gli atti di soft law dunque, per come li conosce il nostro ordinamento, potrebbero avere caratteristiche assimilabili sia agli atti normativi che agli atti amministrativi generali, risultando così difficile la loro collocazione all'interno dell'ordinamento giuridico e quindi la determinazione dei loro effetti.

Per cercare di risolvere l'annosa questione è opportuno fare un passo indietro, abbandonare il C.A.D. per passare a considerare il d.lgs. n. 50/2016, il vigente codice dei contratti pubblici, che nel nostro ordinamento rappresenta il primo esempio di deregolamentazione attuativa.

Il nuovo Codice dei Contratti Pubblici infatti, sin dalla sua formulazione originale (è stato da ultimo modificato dal decreto correttivo n. 56 del 2017) ha demandato all'Autorità Nazionale Anti Corruzione l'emanazione di linee guida attuative della normativa in materia di appalti, conferendole un preciso compito di regolamentazione attuativa della disciplina generale dettata dal d.lgs. 50/2016.

L'utilizzo di questo nuovo strumento di soft law, ha sollevato alcuni dubbi in ordine al carattere precettivo e vincolante delle linee guida e alla loro natura giuridica.

Su espressa richiesta dell’A.N.A.C., il Consiglio di Stato ha emesso un parere con l'obiettivo di chiarire la natura giuridica degli atti di soft law, con particolare riferimento alle linee guida attuative emanate dall’Authority. Il Consiglio di Stato dunque, nel parere n. 1767/2016, oltre a distinguere tra linee guida vincolanti e non vincolanti, ne esclude la valenza normativa e le qualifica come atti amministrativi generali che appartengono al genus degli atti di regolazione delle Autorità Amministrative Indipendenti seppur con specifiche peculiarità.

Secondo il Consiglio di Stato, tali interventi regolativi, sarebbero giustificati dall'elevato tecnicismo della materia che andrebbero a regolare e che richiede un grado di puntualità e dettaglio incompatibile con gli atti legislativi.

Nonostante ci si trovi davanti ad atti di natura non normativa, viene comunque riconosciuto alle linee guida emanate dall'A.N.A.C. un carattere vincolante che non lascia spazio all'esercizio di valutazioni discrezionali in fase applicativa, con la conseguenza che la violazione dei precetti da esse fornite rendono l'atto amministrativo, adottato in violazione, illegittimo. Si tratta allora di una forma di regolamentazione attuativa che non rientra formalmente tra gli atti normativi, ma che esplica gli stessi effetti in termini di potere vincolante sia nei confronti delle Pubbliche Amministrazioni che dei privati.

Se da un lato, dunque, ci troviamo di fronte ad un atto amministrativo vincolante, che incide nella sfera del cittadino, dall'altro è importante capire qual è la tutela nei confronti di una eventuale lesione di questa sfera, direttamente determinata dalla applicazione delle linee guida.

Se le linee guida fossero considerate atti amministrativi generali, ne deriverebbe la loro impugnabilità innanzi al giudice amministrativo sia in via diretta, qualora contenessero delle clausole direttamente lesive o, viceversa, unitamente all'atto lesivo attuativo dell'atto generale. In questa seconda ipotesi si pone il problema dell'individuazione del giudice territorialmente competente a conoscere e giudicare sull'illegittimità dell'atto lesivo impugnato e dell'atto amministrativo generale presupposto.

Il codice del processo amministrativo di cui al D.lgs. 2 luglio 2010 n.104, nel fissare all'art. 13 le regole generali in materia di competenza, prevede al comma 1 che sulle controversie riguardanti provvedimenti e atti delle pubbliche amministrazioni è inderogabilmente competente il tribunale amministrativo regionale nella cui circoscrizione territoriale esse hanno sede. Dunque, dal momento che l'atto impugnato è quello attuativo dell'atto amministrativo generale, sarebbe competente il tribunale amministrativo del luogo presso cui ha sede l'amministrazione che ha emanato l'atto lesivo. Tuttavia, l'art. 13 al comma 4-bis pone una importante deroga al principio secondo cui la competenza territoriale relativa al provvedimento da cui deriva l'interesse a ricorrere attrae a sé anche quella relativa agli atti presupposti dallo stesso provvedimento, quando prevede che tale principio non si applica in presenza di atti presupposti che siano atti normativi o generali, per la cui impugnazione restano fermi gli ordinari criteri di attribuzione della competenza.

Anche la giurisprudenza, nell'interpretazione del dettato normativo del comma 4-bis, ha chiarito che, <<in ipotesi di impugnazione di atti generali o normativi, insieme agli atti applicativi o conseguenziali, la competenza territoriale per l'intera controversia va attribuita al giudice cui spetta la cognizione dell'atto generale o normativo>> (Consiglio di Stato, sez. III, 25 ottobre 2017 n. 4930).

A tale conclusione si può giungere riflettendo sul fatto che gli effetti lesivi sono comunque prodotti dall'atto generale, e tale lesività va ad incidere nella sfera giuridica personale quando l'atto generale presupposto trova attuazione con l'atto applicativo (SANDULLI).

Perciò, nell'impugnazione di un atto consequenziale di uno generale, in cui si contesta un'illegittimità che è direttamente dipendente dalla sua conformità all'atto generale o normativo di cui è attuazione, la competenza è del giudice dell'atto generale poichè nella pretesa nei confronti dell'atto generale è ricompresa anche quella che si eserciterebbe nei confronti dell'atto attuativo. Inoltre, secondo il prevalente orientamento giurisprudenziale, <<una soluzione diversa sarebbe irragionevole in sé, alla luce dei principi di economicità, satisfattività ed effettività della tutela, nonché irragionevole rispetto all'esigenza di congiunta trattazione manifestata dallo stesso legislatore per il caso di presupposizione avente ad oggetto atti individuali>> (Consiglio di Stato, sez. IV, 29 novembre 2017 n. 5602).

Alla luce di tali considerazioni restano comunque molti interrogativi e zone d'ombra, in materia di natura giuridica della soft law, prima fra tutte quella relativa alla possibilità di considerare le linee guida che saranno emanate dall'AgID, per l'attuazione del C.A.D come atti amministrativi generali vincolanti al pari delle linee guida ANAC.

L'interrogativo nasce dal fatto che il Consiglio di Stato, nell'argomentazione relativa alla natura giuridica delle linee guida ANAC e al loro carattere vincolante, parte dal presupposto che esse siano emanate da un'Autorità Amministrativa Indipendente a cui sono affidati poteri di emanazione di atti regolatori e linee guida, e che è proprio la natura non politica, anzi tecnico-amministrativa di A.N.A.C. come Autorità indipendente, ad assicurare idonee garanzie procedimentali nell'adozione di tali atti, arrivando a rispettare un principio di legalità procedimentale, che, in difetto di quello sostanziale, può fare sì che le linee guida, pur restando atti amministrativi generali non normativi, assumano carattere vincolante di tipo regolatorio.

AgID però, a differenza di A.N.A.C. non rientra nel novero delle Autorità Amministrative Indipendenti, con tutte le caratteristiche di cui sopra, essendo una agenzia governativa, quindi di natura politica per espressa previsione statutaria, direttamente controllata dal Governo e sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato. Non sembrerebbe dunque avere quei requisiti di indipendenza dal potere politico che invece hanno le Autorità indipendenti.

È pur vero però che l'art. 71 del Codice dell'Amministrazione Digitale, nel delegare ad AgID l'adozione delle regole tecniche attuative, prevede che l'Agenzia debba procedere, prima dell'adozione, alla consultazione pubblica, e debba successivamente acquisire il parere del Garante

Privacy e della Conferenza unificata, istituendo così un procedimento di adozione della soft law, simile a quello garantito da A.N.A.C.

Resta da capire allora, se in presenza di idonee garanzie di tipo procedimentale, gli atti di soft law emanati da AgID per l'attuazione del Codice dell'Amministrazione Digitale possano essere considerate della stessa natura giuridica delle linee guida ANAC, e produrre gli stessi effetti vincolanti all'interno dell'ordinamento, e se il principio di legalità procedimentale diventerà l'elemento salvagente della soft law nel nostro ordinamento.

1.3. Il nuovo ambito di applicazione soggettivo del CAD

In base al riformulato art. 2, comma 2 del CAD, le disposizioni del Codice si applicano nella loro totalità ad una molteplicità di enti:

a) alle Pubbliche Amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione; si chiarisce che, in base al citato articolo 1, comma 2, del Decreto Legislativo 30 marzo 2001, n. 165, per <<Amministrazioni Pubbliche>> dobbiamo intendere 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 l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; si chiarisce che per <<società quotate>>, in base all'art. 2, comma 1, lett. p), del D.Lgs. 19 agosto 2016, n. 175, occorre intendere le società a partecipazione pubblica che emettono azioni quotate in mercati regolamentati, nonchè le società che hanno emesso, alla data del 31 dicembre 2015, strumenti finanziari, diversi dalle azioni, quotati in mercati regolamentati e, infine, le società partecipate dalle une o dalle altre, salvo che le stesse siano anche controllate o partecipate da amministrazioni pubbliche;

c) alle società a controllo pubblico, come definite nel D.Lgs. 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b); si chiarisce che in base al D.Lgs. 19 agosto 2016, n. 175, art. 2,

comma 1, lett. m), sono da definirsi <<società a controllo pubblico>> le società in cui una o più amministrazioni pubbliche esercitano poteri di controllo ai sensi della lettera b) del medesimo art. 2, comma 1, lettera che, nello specifico, definisce la situazione di <<controllo>> come la situazione descritta nell'articolo 2359 del codice civile, specificando, inoltre, che il controllo può sussistere anche quando, in applicazione di norme di legge o statutarie o di patti parasociali, per le decisioni finanziarie e gestionali strategiche relative all'attività sociale è richiesto il consenso unanime di tutte le parti che condividono il controllo.

Non innovando rispetto al passato, le disposizioni del Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II (dal titolo <<Documento informatico, firme elettroniche, servizi fiduciari e trasferimenti di fondi>>), la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV (dal titolo <<Trasmissione informatica dei documenti>>), l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto.

Ulteriore importante specificazione all'interno dell'art. 2, comma 4, parzialmente innovato dal D.Lgs. n. 217/2017, riguarda poi l'applicabilità del CAD agli <<organismi di diritto pubblico>>: in particolare, ad essi si applicano le disposizioni di cui al capo V (dal titolo <<Dati delle Pubbliche Amministrazioni, identità digitali , istanze e servizi online>>), concernenti l'accesso ai documenti informatici e la fruibilità delle informazioni digitali. Volendo chiarire la portata della definizione di <<organismo pubblico>>, in base all'art. 3, comma 1, lett. d), del D.Lgs. n. 50/2016 (<<Codice dei contratti pubblici>>), bisogna intendere qualsiasi organismo, anche in forma societaria, il cui elenco non tassativo è contenuto nell'allegato IV del medesimo Codice, ovvero: Mostra d'oltremare S.p.A., Ente nazionale per l'aviazione civile – ENAC, Società nazionale per l'assistenza al volo S.p.A. - ENAV ANAS S.p.A., Consip S.p.A. (quando Consip agisce in qualità di centrale di committenza per le autorità sub-centrali), Consorzi per le opere idrauliche, Università statali, gli istituti universitari statali, i consorzi per i lavori interessanti le università, Istituzioni pubbliche di assistenza e di beneficenza, Istituti superiori scientifici e culturali, osservatori astronomici, astrofisici, geofisici o vulcanologici, Enti di ricerca e sperimentazione, Enti che gestiscono forme obbligatorie di previdenza e di assistenza, Consorzi di bonifica, Enti di sviluppo e di irrigazione, Consorzi per le aree industriali, Comunità montane, Enti preposti a servizi di pubblico interesse, Enti pubblici preposti ad attività di spettacolo, sportive, turistiche e del tempo libero, Enti culturali e di promozione artistica.

Senza innovare rispetto al passato, il CAD continua ad essere applicato nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia

di protezione dei dati personali approvato con D.Lgs. n. 30 giugno 2003, n. 196. In materia, occorre sottolineare che la Legge n. 163 del 25 ottobre 2017 ha delegato il Governo al recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea. L'art. 13 demanda al Governo il compito di adottare i decreti legislativi per adeguare entro sei mesi il quadro normativo nazionale (quindi il <<Codice Privacy>> di cui al D.Lgs. n. 196/2003) al Regolamento UE 2016/679 (GDPR), che, a decorrere dal 25 maggio 2018, diverrà esecutivo in tutti i Paesi membri e detterà una nuova disciplina su scala continentale in tema di protezione dei dati personali.

Analizzando ora il comma 6 dell'art. 2 del CAD, come modificato dal correttivo 2017, esso dispone la non applicazione del Codice limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile.

Le disposizioni del Codice, invece, si applicano al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico.

Particolare approfondimento merita, poi, la materia tributaria, per la quale si rimanda al prossimo paragrafo.

1.4. L'estensione dell'ambito di applicazione oggettivo: il settore tributario

Il C.A.D. conteneva alcune disposizioni indubbiamente di ostacolo alla effettiva applicazione delle sue norme alla materia tributaria. Ostacoli rimossi con il correttivo di cui al D.Lgs. n. 217/2017 a decorrere dal 27 gennaio 2018.

In particolare, l'art. 2, comma 6, ante riforma, indicava tra le materie escluse dall'applicazione del CAD proprio le <<attività e funzioni ispettive e di controllo fiscale>>.

A seguito delle modifiche al CAD introdotte dal D.Lgs n. 217/2017, le <<attività e funzioni ispettive e di controllo fiscale>> non rientrano più tra le materie sottratte all'applicazione del Codice.

Il nuovo comma 6-bis dell'art. 2 sancisce poi, in maniera specifica, l'applicabilità immediata del CAD agli atti di liquidazione, rettifica, accertamento e di irrogazione delle sanzioni di natura tributaria, distinguendoli da quelli relativi alle attività di ispezione e controllo fiscale in senso proprio per i quali, invece, si rinvia ad un DPCM o DM per la definizione delle specifiche modalità e termini di applicazione.

La riforma del CAD comporta, inoltre, l'introduzione di un nuovo comma 1-quater all'art. 6, in base al quale i soggetti a cui si applica il Codice (Amministrazioni, gestori di pubblico servizio in

relazione ai servizi di pubblico interesse, società a controllo pubblico) possono notificare direttamente anche alle persone fisiche presso i domicili digitali i propri atti, compresi i verbali relativi alle sanzioni amministrative, gli atti impositivi di accertamento e di riscossione e le ingiunzioni di cui al R.D. n. 639/1910. Dal necessario coordinamento della disposizione in esame con la specifica norma tributaria di cui all'art. 60 del D.P.R. n. 600/1973 consegue che la notifica degli atti tributari alle persone fisiche rimane condizionata alla previa autorizzazione da parte del contribuente e limitata esclusivamente alle ipotesi di perfezionamento della notifica. Al contrario, se la casella del contribuente risulta satura ovvero non valida o non attiva, l'Ente impositore è tenuto a procedere alla notificazione dell'atto in base all'artt. 137 e seguenti del Codice di Procedura Civile (con esclusione dell'art. 149-bis c.p.c.) ovvero a mezzo posta ordinaria con raccomandata a/r in base alla L. n. 890/1982.

Sempre in materia tributaria, altra importante novità della modifica al CAD operata con il D.Lgs. n. 217/2017 è contenuta nell'art. 5, che vede l'inserimento dei commi 2-ter, 2-quater e 2-quinquies. L'articolo disciplina la piattaforma tecnologica finalizzata a permettere ai cittadini e imprese di effettuare pagamenti verso la Pubblica Amministrazione: pagoPA. Essa è un ecosistema di regole, standard e strumenti definiti dall'Agenzia per l'Italia Digitale e accettati dalla Pubbliche Amministrazioni, dalle Banche, dalle Poste e dagli altri istituti di pagamento (PSP – prestatori di servizi di pagamento) aderenti all'iniziativa per permettere ai cittadini di pagare in formato digitale attraverso tale Nodo nazionale. Volendo esemplificare, attraverso pagoPA è possibile effettuare i pagamenti direttamente sul sito o sull'app dell'Ente aderente (il comune di residenza, ad esempio) o attraverso i canali (online e fisici) di banche e altri Prestatori di Servizio a Pagamento (PSP), come le agenzie della banca di riferimento, l'home banking della banca di riferimento (dotato dei loghi CBILL o pagoPA), gli sportelli ATM della banca di riferimento (se abilitati), i punti vendita di SISAL, Lottomatica e Banca 5 e le Poste, se la Pubblica Amministrazione verso cui versare ha attivato anche tale possibilità. Il sistema pagoPA permette quindi di pagare tributi, tasse, utenze, rette, quote associative, bolli e qualsiasi altro tipo di pagamento verso le Pubbliche Amministrazioni centrali e locali, ma anche verso altri soggetti, come le aziende a partecipazione pubblica, le scuole, le università, le ASL.

Con i su citati nuovi commi 2-ter e 2-quater dell'art. 5 CAD, è disposto che le Pubbliche Amministrazioni, i gestori di pubblici servizi e le società a controllo pubblico devono consentire al cittadino di effettuare, tramite la piattaforma pagoPA, anche i pagamenti spontanei relativi alle entrate tributarie dei Comuni e degli altri enti locali, IMU e TASI. Con il comma 2-quater tuttavia si precisa che resta fermo il sistema di versamento unitario di crediti e debiti relativi a imposte, contributi INPS e altre somme a favore dello Stato, delle regioni e degli enti previdenziali (F24)

fino all'adozione di un DPCM che fisserà, anche in maniera progressiva, le modalità tecniche per l'effettuazione dei pagamenti tramite piattaforma anche in campo tributario e contributivo. In attesa del DPCM, sappiamo che questi pagamenti, finora esclusi da pagoPA, dovranno transitare dal Nodo. Ogni informazione sui pagamenti gestita da pagoPA sarà messa a disposizione del Ministero dell'Economia e delle Finanze – Dipartimento Ragioneria generale dello Stato, come recita il citato comma 2-quinquies, ultimo comma aggiunto all'art. 5 CAD dal decreto di riforma.

Volendo trarre delle conclusioni, è chiara la volontà del legislatore di far confluire in modo progressivo tutti i pagamenti a favore della Pubblica Amministrazione sul Nodo nazionale dei pagamenti, abbandonando ogni altro sistema, ancorché elettronico (POS, F24), con l'obiettivo di avere un unico punto di monitoraggio e controllo delle entrate della PA e non solo quello di favorire la diffusione dei pagamenti digitali.

1.5 Le novità in materia di acquisti ad oggetto informatico e riuso software

L'acquisto di beni e servizi informatici da parte delle pubbliche amministrazioni è un tema assai caldo, negli ultimi anni oggetto di numerosissimi interventi legislativi.

Già la legge n. 218/15 (cd. legge di stabilità 2016) ha previsto che <<al fine di garantire l'ottimizzazione e la razionalizzazione degli **acquisti di beni e servizi informatici e di connettività**, le PA provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti>> (art. 512, nel testo attualmente vigente).

Residua in capo alle PA la possibilità di approvvigionarsi al di fuori di Consip, esclusivamente a seguito di apposita autorizzazione motivata dell'organo di vertice amministrativo, qualora il bene o il servizio non fosse disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione, o in casi di necessità ed urgenza comunque funzionali ad assicurare la continuità della gestione amministrativa (art. 516), lasciando spazio, dunque, solo per queste ipotesi, all'applicabilità della procedura negoziata senza previa pubblicazione di un bando di gara di cui all'art. 63 del D.Lgs. n. 50/2016, recante nuovo codice dei contratti pubblici.

Successivamente, la cd. Legge di bilancio 2017, ovvero la legge 11 dicembre 2016 n. 232, ha apportato alcune modifiche alla suddetta disciplina, prevedendo in particolare che, per i beni e servizi la cui acquisizione riveste particolare rilevanza strategica secondo quanto indicato nel Piano triennale per l'informatica nella Pubblica Amministrazione, le amministrazioni statali, centrali e periferiche, ad esclusione di qualche eccezione, tra cui gli istituti e le scuole di ogni ordine e grado, le istituzioni educative e le istituzioni universitarie, ricorrono a Consip Spa, nell'ambito del

Programma di razionalizzazione degli acquisti della pubblica amministrazione del Ministero dell'economia e delle finanze, potendo anche ricorrere al supporto della stessa Consip nell'individuazione di specifici interventi di semplificazione, innovazione e riduzione dei costi dei processi amministrativi (nuovo art. 514-bis, legge di stabilità 2016).

Sul tema, è intervenuto anche il correttivo 2018 al CAD, laddove ha introdotto un ulteriore compito tra quelli affidati al **responsabile per la transizione digitale**, ufficio che, come si dirà nel prosieguo, acquista un ruolo sempre più forte e pregnante.

A tale figura, infatti, è stato attribuito, tra gli altri, il compito relativo alla <<pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale>> (art. 17 comma 1 lett. j-bis, CAD).

Per quanto concerne **l'acquisto pubblico di programmi informatici, i cd. *software***, come è noto l'art. 68 CAD già prevedeva l'analisi comparativa delle soluzioni disponibili, che consiste nel fatto che le pubbliche amministrazioni, prima di procedere all'acquisto secondo le procedure di cui al codice di cui al decreto legislativo n. 50 del 2016, effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base di specifici criteri elencati al comma 1-bis. Soltanto ove da tale valutazione comparativa risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso.

Se tale disposto è stato confermato dal correttivo 2018, così non è accaduto per il successivo art. 69, recante disciplina del **riuso del *software* della pubblica amministrazione**, che è stato modificato in senso favorevole alle amministrazioni sviluppatrici.

E infatti, ai sensi dell'art. 69 comma 1, che non è stato interessato dalla modifica legislativa, per le ipotesi di software sviluppato per conto della pubblica amministrazione, <<le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di **rendere disponibile il relativo codice sorgente**, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali>> (art. 69, comma 1, CAD).

Il correttivo 2018, in prima battuta ha cancellato l'obbligo di inserire nei capitolati o nelle specifiche di progetto <<che i programmi ed i servizi ICT appositamente sviluppati per conto e a spese

dell'amministrazione siano conformi alle specifiche tecniche di SPC definite da AgID>>, in ossequio all'autonomia organizzativa della singola amministrazione committente.

Inoltre, ha previsto *ex novo* che i capitolati e le specifiche di progetto prevedano espressamente che <<l'amministrazione committente sia sempre **titolare di tutti i diritti sui programmi e i servizi delle tecnologie dell'informazione e della comunicazione, appositamente sviluppati per essa**>>, salvo che ciò risulti eccessivamente oneroso (art. 69 comma 2).

In secondo luogo, sempre al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, <<il codice sorgente, la documentazione e la relativa descrizione tecnico funzionale>> di tutte le soluzioni informatiche sviluppate per conto della pubblica amministrazione, dovranno essere pubblicati attraverso una o più piattaforme individuate dall'AgID con proprie Linee guida (art. 69, comma 2-bis).

A tal proposito, si segnala che sono attualmente in fase di consultazione pubblica le "**Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni"**, redatte da un gruppo di lavoro costituito da componenti dell'AgID e del Team per la Trasformazione Digitale, proprio in attuazione degli articoli 68 e 69 CAD, che, tra le altre attribuzioni, dovranno definire e regolamentare uno specifico contenitore nel quale confluiranno le sopra dette componenti a codice sorgente aperto, per essere rese disponibili alle altre pubbliche amministrazioni.

Tali linee guida sostituiranno la Circolare AgID 6 dicembre 2013 n. 63, recante "Linee guida per la valutazione comparativa prevista dall'art. 68 del D.Lgs. 7 marzo 2005, n. 82 Codice dell'Amministrazione digitale", attualmente documento di riferimento per le pubbliche amministrazioni che intendono procedere all'acquisto di *software*.

CAPITOLO 2
CARTA DELLA CITTADINANZA DIGITALE E DIRITTI DEL CITTADINO

2.1. Diritto all'uso delle nuove tecnologie

Con la novella del 2018 il legislatore ha previsto all'art. 4 del Dlgs. 13 dicembre 2017 n. 217 l'introduzione nell'art. 3 del CAD (Diritto all'uso delle tecnologie) di alcune specificazioni. In particolare si è ritenuto opportuno specificare che chiunque abbia il diritto di usare le soluzioni e gli strumenti delle tecnologie previste dal CAD in modo accessibile ed efficace. Con ciò, evidentemente, si è ritenuto di voler scongiurare il rischio che la fruizione dei servizi pubblici on-line sia garantita solo formalmente, essendo sostanzialmente preclusa ad alcune categorie di utenti.

Per comprendere la ratio della modifica normativa pare utile ricordare che ai sensi dell'art. 2 della Legge per accessibilità deve intendersi <<la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, **anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari**>>.

Il legislatore ha, inoltre, voluto anche precisare che il diritto all'uso delle nuove tecnologie in modo accessibile ed efficace oltre che ai fini della partecipazione al procedimento amministrativo deve essere garantito anche ai fini dell'esercizio dei diritti di accesso.

Infine l'art. 4 del Dlgs. n. 217/2017 ha disposto l'abrogazione dei commi 1-quater, 1-quinquies e 1-sexies dell'art. 3 del previgente CAD in quanto la relativa disciplina risulta essere stata assorbita dalla nuova disciplina dell'identità e del domicilio digitale (art. 3 bis del CAD).

Giunge così al completamento quel processo di graduale ampliamento del diritto all'uso delle nuove tecnologie nei confronti della P.A. che poteva essere inizialmente fatto valere solo da cittadine e imprese nei confronti delle amministrazioni statali. Successivamente con le modifiche introdotte dal Dlgs. 4 aprile 2006, n. 159 e l'introduzione nell'art. 3 del comma 1-bis si estendeva tale diritto anche alle amministrazioni regionali e locali nei limiti delle risorse tecnologiche ed organizzative disponibili e nel rispetto della loro autonomia normativa. Il Dlgs. 30 dicembre 2010, n. 235 disponeva poi l'abrogazione del comma 1-bis dell'art. 3 estendendo l'ambito del diritto in oggetto ai rapporti con i soggetti di cui all'art. 2, comma 2 del CAD, vale a dire le <<pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311>>.

Infine, recependo le osservazioni di una parte della dottrina che riteneva discriminatoria la previsione del diritto in oggetto esclusivamente in favore di cittadini e imprese, con esclusione di coloro che, pur non avendo la cittadinanza italiana, si trovassero ad interagire con la pubblica amministrazione italiana, il legislatore ha modificato l'originaria previsione dell'art. 3 del CAD sostituendo all'espressione restrittiva <<cittadini e imprese>> quella omnicomprensiva <<chiunque>>.

2.2. Identità e domicilio digitale

Significative modifiche sono state apportate dall'art. 5 del Dlgs. 13 dicembre 2017 n. 217 all'art. 3 bis del CAD. In primo luogo il legislatore della novella ha sostituito l'originaria rubrica dell'art. 3 bis del Cad, <<Domicilio digitale delle persone fisiche>>, con <<Identità digitale e Domicilio digitale>> e ciò in quanto

la disposizione è stata notevolmente ampliata al fine di realizzare una <<disciplina organica e sistematica dei diritti di cittadinanza digitale>> (Relazione illustrativa, pag. 4).

Ed in effetti, come può evincersi dal disposto dell'art. 3 bis, comma 1, viene ora riconosciuto il diritto di chiunque di accedere ai servizi online offerti dalle pubbliche amministrazioni tramite la propria identità digitale. Tale disposizione va raccordata con la definizione contenuta nell'art. 1, comma u-quater, ai sensi del quale per identità digitale deve intendersi <<la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme di dati raccolti e registrati in forma digitale secondo le modalità fissate dal CAD all'art. 64>>.

L'originario primo comma dell'art. 3 bis è ora confluito nel comma 1 bis del medesimo articolo con due rilevantissime modifiche. Innanzitutto la facoltà di eleggere il proprio domicilio digitale non è riconosciuta in modo restrittivo ai soli cittadini, ma a chiunque, e ciò in linea con quanto si è già esposto nel paragrafo precedente. In secondo luogo tale elezione che nella disciplina previgente avveniva mediante indicazione al comune di residenza, dovrà essere effettuata mediante iscrizione nell'<<Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese>> istituito dall'art. 6 quater del CAD.

Ciò che per qualunque persona fisica è una mera facoltà, è invece un obbligo sia per le pubbliche amministrazioni sia per i professionisti tenuti all'iscrizione in albi ed elenchi e per i soggetti tenuti all'iscrizione nel registro delle imprese.

Tuttavia, a differenza di quanto previsto per le persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese, l'elezione del domicilio digitale dovrà avvenire per i professionisti e per le imprese mediante iscrizione nell'<<Indice nazionale dei domicili digitali delle imprese e dei professionisti>> (INI-PEC) di cui all'art. 6 bis e per le pubbliche amministrazioni mediante l'iscrizione nell'<<Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi>> (iPA).

Viene, inoltre, precisato al comma 1-ter che l'elezione del domicilio digitale da parte delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione negli albi professionali o nel registro delle imprese dovrà avvenire secondo le modalità stabilite con le linee guida. Le persone fisiche possono altresì eleggere il domicilio digitale avvalendosi del servizio di cui all'articolo 64-bis (Accesso telematico ai servizi della Pubblica Amministrazione).

L'art. 5 del Dlgs. 13 dicembre 2017 n. 217 ha, inoltre, disposto l'abrogazione del secondo comma del previgente art. 3 del CAD ai sensi del quale il domicilio digitale eletto dalle persone fisiche avrebbe dovuto essere inserito nell'Anagrafe nazionale della popolazione residente-ANPR. Tale abrogazione si è resa necessaria a seguito dei ritardi nello sviluppo e nella implementazione dell'ANPR (Anagrafe nazionale della popolazione residente) e al fine di evitare che questo ritardo si traduca in un ostacolo all'immediato utilizzo del domicilio digitale da parte degli utenti e ai risparmi che ne derivano sia per questi ultimi sia per la

pubblica amministrazione. Ciò comporta che le P.A. potranno subito avvalersi dei domicili digitali eletti in base alle linee guida o mediante il servizio di cui all'art. 64 bis del CAD, senza dover attendere l'inserimento dei predetti nell'ANPR, il che appare del tutto condivisibile anche se, come ha notato il Consiglio di Stato nel proprio parere, <<la scelta operata dall'Amministrazione non dovrà rallentare ulteriormente i tempi di effettiva implementazione dell'ANPR, atteso che la realizzazione dell'Anagrafe, prevista dal Codice sin dalla novella recata dall'art. 2 del d.l. n. 179 del 18 ottobre 2012, costituisce in ogni caso un importante tassello del complessivo processo di digitalizzazione del Paese>> (Adunanza della Commissione speciale del 4 ottobre 2017, numero affare 01654/2017).

Sul versante della lotta al digital-divide appare molto significativa la disposizione di cui al comma 3 bis dell'art. 3 del CAD. Il legislatore, consapevole del fatto che la diffusione dei domicili digitali tra le persone fisiche potrà avvenire solo gradualmente, ha previsto le modalità con le quali le pubbliche amministrazioni potranno (e dovranno) gestire tale transizione, disponendo che con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per la semplificazione e la pubblica amministrazione, sentiti AgID e il Garante per la protezione dei dati personali e acquisito dalla Conferenza unificata, dovranno essere stabilite le modalità con le quali i documenti predisposti in digitale dalle P.A. potranno essere consegnati a coloro che non sono in grado di accedere direttamente al domicilio digitale. Con lo stesso decreto dovrà essere fissata la data a decorrere dalla quale le comunicazioni delle P.A. dovranno avvenire esclusivamente in forma elettronica anche a coloro che non abbiano eletto il domicilio digitale e le modalità con le quali sarà messo a disposizione di questi ultimi un domicilio digitale.

Il comma 4 bis dell'art. 3 del CAD precisa, inoltre, che in assenza di domicilio digitale potranno essere effettuate comunicazioni mediante invio a mezzo posta ordinaria o raccomandata con avviso di ricevimento di copia analogica sottoscritta con firma autografa sostituita a mezzo stampa di documenti informatici sottoscritti con firma digitale o firma elettronica qualificata o avanzata da conservare nei propri archivi.

Infine il comma 4 quinquies del CAD, come modificato dalla novella del 2018, dispone che ove venga eletto un domicilio digitale con modalità diverse da quelle previste dalle linee guida o dall'art. 64 bis del CAD non sarà possibile opporre eccezioni relative alla forma e alla data della spedizione e del ricevimento delle comunicazioni o notificazioni effettuate presso il domicilio speciale eletto ex art. 47 c.c.

2.3. Effettuazione dei pagamenti con modalità informatiche

In linea con gli obiettivi definiti dalla legge delega e al fine di <<ridefinire e semplificare i procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese" (Legge 7 agosto 2015, n. 124, art. 1, comma 1, lett. b) l'art. 5 del CAD prevede che le P.A. debbano accettare i pagamenti in forma elettronica.

In particolare, l'art. 5 del CAD prevede al comma secondo la creazione di una piattaforma tecnologica gestita dall'AgID per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati per la gestione del processo di pagamento elettronico.

Rimane comunque ferma ai sensi del primo comma dell'art. 5 la possibilità per le P.A. di accettare anche altre forme di pagamento elettronico ivi incluso il pagamento mediante uso del credito telefonico.

Con la novella del 2018 il legislatore ha ritenuto opportuno estendere l'ambito di applicazione del pagamento elettronico anche al versamento spontaneo delle entrate tributarie dei comuni e degli altri enti locali (art. 2 bis del D.L. 22 ottobre 2016, n. 193, convertito con modificazioni dalla Legge 1° dicembre 2016, n. 225). Pertanto questi ultimi saranno tenuti a consentire ai sensi del comma 2 ter dell'art. 5 del CAD che tali versamenti spontanei vengano effettuati tramite la piattaforma di cui al precedente comma secondo dell'art. 5.

Il successivo comma 2 quater dell'art. 5 (introdotto dalla novella del 2018) statuisce l'obbligo per i prestatori di servizi di pagamento abilitati di eseguire i pagamenti in favore delle pubbliche amministrazioni mediante la piattaforma prevista dal precedente comma 2. Tuttavia tale modalità è prevista come alternativa all'utilizzo dello strumento dell'F24 (ex art. 17 e seguenti del Dlgs. 9 luglio 1997, n. 241, Capo III) fino all'adozione di un DPCM, su proposta del ministro delegato e di concerto con il ministro dell'economia e delle finanze e con il ministro del lavoro e delle politiche sociali, sentite l'Agenzia delle Entrate e l'AgID, nel quale vengano fissate le modalità tecniche per l'effettuazione in forma elettronica (e tramite la piattaforma di cui al secondo comma dell'art. 5) dei pagamenti tributari e contributivi.

Il correttivo al CAD da ultimo approvato ha, infine, introdotto nell'art. 5 il principio secondo cui la piattaforma di cui al secondo comma del medesimo articolo deve mettere a disposizione anche del Ministero dell'economia e delle finanze – Dipartimento Ragioneria generale dello Stato.

L'art. 5 del CAD come modificato dall'ultimo correttivo, attua in modo sempre più completo gli indirizzi definiti nella legge delega (Legge 7 agosto 2015, n. 124) con particolare riferimento alla previsione della lett. c dell'art. 1, comma 1 volta a garantire <<la piena disponibilità dei sistemi di pagamento elettronico>> nei rapporti con le pubbliche amministrazioni e della lett. d del medesimo comma finalizzata a fare in modo <<che i pagamenti digitali ed elettronici effettuati con qualsiasi modalità di pagamento, ivi incluso l'utilizzo per i micropagamenti del credito telefonico, costituiscano il mezzo principale per i pagamenti dovuti nei confronti della pubblica amministrazione e degli esercenti servizi di pubblica utilità>>.

2.4. Indici nazionali dei domicili digitali

Il nuovo art. 6, che disciplina le comunicazioni tramite i domicili digitali, chiarisce che esse sono effettuate agli indirizzi inseriti negli elenchi di cui agli articoli 6-bis, 6-ter e 6-quater.

Si illustrano, dunque, qui di seguito, i singoli elenchi.

2.4.1 Indice nazionale dei domicili digitali delle imprese e dei professionisti (art. 6-bis)

Si tratta del "Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti", cd. INI-PEC, detenuto presso il Ministero per lo sviluppo economico, e realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali. Il correttivo al CAD lo ha dunque ridenominato "elenco dei domicili digitali delle imprese e dei professionisti (art. 6 comma 1-ter).

Esso raccoglie effettivamente tutti gli indirizzi di PEC delle imprese e dei professionisti presenti sul territorio italiano, in quanto il Registro delle Imprese e tutti gli Ordini e i Collegi professionali sono tenuti a trasferirvi gli indirizzi PEC dei propri iscritti, nonché ad aggiornare i dati forniti nei tempi e nelle modalità stabiliti per legge, garantendo in tal modo la qualità delle informazioni messe a disposizione da INI-PEC.

INI-PEC è accessibile senza necessità di autenticazione tramite il sito web indicepa.gov.it, ed è inserito tra gli elenchi pubblici rilevanti ai fini delle notificazioni telematiche.

2.4.2 Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (art. 6-ter)

L'elenco dei domicili digitali della pubblica amministrazione è l'"Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi", di cui all'articolo 6-ter, il noto IndicePA (www.indicepa.gov.it).

IndicePA, originariamente introdotto dall'art. 57-bis del CAD, è realizzato e gestito da AgID, è un valido ed effettivo elenco pubblico di PEC pubbliche, in quanto le amministrazioni sono tenute ad aggiornare i loro indirizzi con cadenza almeno semestrale, pena la valutazione ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

Tale elenco, tuttavia, già dal 19 agosto 2014 non è più elenco pubblico utilizzabile per le notifiche ex legge n. 53, in quanto espunto dall'elenco tassativo dalla legge n. 114/14, di conversione con modificazioni del D.L. n. 90/2014.

2.4.2 Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese (art. 6-quater)

Si tratta di un elenco nuovo di zecca, che conterrà i domicili eletti da tutti i soggetti privati diversi da imprese e professionisti, che, come sopra detto, non sono solo i cittadini, ma anche i residenti nel nostro paese senza cittadinanza italiana.

Innanzi tutto, per tali soggetti privati rimane comunque la facoltà -e non l'obbligo come è stabilito per imprese, PA e professionisti- di eleggere il proprio domicilio digitale.

In secondo luogo, tale elezione di domicilio sostituisce quella che, nella disciplina previgente, introdotta dal decreto correttivo 26 agosto 2016 n. 179, avveniva mediante indicazione da parte del cittadino, al comune di residenza.

La realizzazione e la gestione dell'Indice sono affidate all'AgID, che vi provvede avvalendosi delle strutture informatiche delle Camere di commercio gia' deputate alla gestione dell'INI-PEC

E' importante rilevare che, per i professionisti iscritti in albi ed elenchi, il domicilio digitale rimane quello inserito in INI-PEC, fermo restando il diritto di eleggerne uno diverso da inserire nell'elenco delle persone fisiche.

Tale elenco dei domicili digitali delle persone fisiche sembra essere tuttavia transitorio: l'ultimo comma dell'art. 6-quater infatti prevede che, al completamento dell'ANPR di cui all'articolo 62, AgID provvederà a trasferirvi i domicili digitali per allora contenuti nell'elenco delle persone fisiche in commento.

2.5 Anagrafe Nazionale della Popolazione Residente

L'art. 62 CAD prevede l'istituzione dell'ANPR, disciplinandola compiutamente sin dal Decreto Legge 18 ottobre 2012 n. 179.

Si tratta di una base di dati di interesse nazionale ai sensi dell'articolo 60, che subentrerà all'Indice nazionale delle anagrafi (INA), all'Anagrafe della popolazione italiana residente all'estero (AIRE), nonché alle anagrafi tenute dai comuni. L'ANPR conterrà altresì l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni.

Tale base di dati sarà sottoposta ad un audit di sicurezza con cadenza annuale, i cui risultati saranno inseriti nella relazione annuale del Garante per la protezione dei dati personali.

L'ANPR dovrà assicurare ai comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, e metterà a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e

transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale.

Il correttivo 2018 ha peraltro aggiunto che il Comune potrà utilizzare direttamente i dati anagrafici eventualmente detenuti localmente e costantemente allineati con ANPR, ma al fine esclusivo di erogare o usufruire di servizi o funzionalità non fornite da ANPR.

L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafici**, ma assicura a tutte le pubbliche amministrazioni l'accesso ai dati contenuti nel proprio elenco.**

Altra nuova previsione del correttivo 2018 è un apposito decreto che dovrà regolamentare l'erogazione di altri servizi resi disponibili dall'ANPR, tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e di morte.

2.6. Diritto a servizi on line semplici ed integrati

L'art. 7 del CAD, come modificato e integrato dal correttivo del 2018, riconosce al comma 1 il diritto di fruire dei servizi erogati dalle pubbliche amministrazione in forma digitale e in modo integrato e anche attraverso dispositivi mobili. Ancora una volta il legislatore ha ritenuto opportuno utilizzare la formula omnicomprensiva "chiunque" al fine di evitare alcun tipo di discriminazione nei confronti delle persone fisiche, non in possesso della cittadinanza italiana, che si trovino ad interagire con le pubbliche amministrazioni italiane. Tuttavia va rilevato che l'art. 65, comma 6, del Dlgs. 13 dicembre 2017, n. 217 ha disposto che il diritto in questione verrà riconosciuto solo a decorrere dalla data di attivazione del punto di accesso di cui all'art. 64 bis del CAD.

Il diritto in questione rappresenta una novità rispetto al testo previgente nel quale è stato sostituito il primo comma. Inoltre con la novella del 2018 si è anche provveduto a modificare la rubrica dell'articolo in questione da "Qualità dei servizi resi e soddisfazione dell'utenza" in "Diritto a servizi on-line semplici e integrati". Con ciò si è evidentemente voluta rafforzare la natura di "Carta della cittadinanza digitale" della prima sezione del CAD.

Al fine di evitare eccessivi oneri a carico delle amministrazioni periferiche l'art. 7, comma 01, prevede che le pubbliche amministrazioni possano avvalersi del punto di accesso telematico di cui all'art. 64bis del CAD, attivato presso la Presidenza del Consiglio dei Ministri.

Il secondo e il terzo comma dell'art. 7, inoltre, impongono alle pubbliche amministrazioni due importanti obblighi. Si tratta in particolare dell'obbligo di effettuare una preventiva analisi delle reali esigenze degli utenti al fine di riorganizzare e aggiornare i servizi offerti (comma 2) e dell'obbligo di testare il grado di soddisfazione degli utenti anche in termini di fruibilità, accessibilità e tempestività del servizio reso (comma 3).

L’importanza del monitoraggio previsto dalle disposizioni in commento è evidente atteso che solo un costante controllo del grado di soddisfazione degli utenti può consentire alle pubbliche amministrazioni di migliorare costantemente la qualità dei servizi offerti agli utenti.

La previsione degli importanti obblighi precedentemente esposti trova una adeguata tutela nel riconoscimento agli utenti a tutela dei propri diritti del diritto di rivolgersi al difensore civico digitale previsto dall’art. 17, ma anche del diritto di avvalersi del ricorso per l'efficienza delle amministrazioni e dei concessionari di servizi pubblici di cui al Dlgs. 20 dicembre 2009, n. 198.

2.7 Lo SPID

Particolarmente rilevante appare la disciplina, contenuta nell’art. 64 del CAD, in relazione al Sistema Pubblico per la gestione dell’identità digitale di cittadini e imprese (c.d. SPID). Lo SPID è gestito dall’Agenzia per l’Italia digitale ed è costituito da un sistema misto pubblico-privato volto a consentire l’identificazione degli utenti ai fini del loro accesso ai servizi in rete offerti dalle pubbliche amministrazioni.

Al momento il sistema di identificazione predisposto dall’AGID si è sostanziato in un PIN unico che viene rilasciato dagli enti certificatori accreditati presso l’Agenzia per l'Italia Digitale previa verifica dell’identità dei richiedenti.

Ai sensi del comma 2 quater dell’art. 64 i tempi e le modalità di adozione da parte delle pubbliche amministrazioni del sistema SPID vengono previsti in un apposito decreto del Presidente del Consiglio dei ministri, su proposta del ministro delegato per l’innovazione tecnologica e del ministro per la pubblica amministrazione e la semplificazione, di concerto con il ministro dell’economia e delle finanze, sentito il parere del Garante per la protezione dei dati personali. Il decreto in questione è stato emanato il 24 ottobre 2014 e ha indicato come soggetti che partecipano allo SPID cinque categorie: i gestori dell'identità digitale, i gestori degli attributi qualificati, i fornitori di servizi, l'Agenzia e gli utenti (art. 3 del DPCM).

Per gestori dell’identità digitale devono intendersi tutti i soggetti pubblici o privati accreditate allo SPID che assegnano, rendono disponibili e gestiscono gli attributi utilizzati da ciascun utente al fine della sua identificazione informatica di gestori di servizio pubblico. Specifica il DPCM in esame che nell’esercitare le citate funzioni questi soggetti assumono la veste di gestori di un servizio pubblico con tutti gli obblighi e gli oneri connessi e consequenziali.

Categoria peculiare è, invece, quella dei gestori degli attributi qualificati. Si tratta di quei soggetti che possono certificare per legge una qualifica. In tale categoria possono, per esempio, farsi rientrare gli ordini professionali o nell’ambito delle pubbliche amministrazioni quei soggetti che possono certificare il qualifica di responsabile unico del procedimento conferita ad un determinato funzionario o l’appartenenza di un funzionario al ruolo dirigenziale.

Si distinguono dagli attributi qualificati i c.d. attributi elementari (o non qualificati) i quali ultimi sono conservati dai gestori di identità digitale e si distinguono in attributi identificativi (nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione) e attributi secondari (il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonchè eventuali altri attributi individuati dall'Agenzia,

funzionali alle comunicazioni). Va notato che, in ogni caso, ai sensi del comma 2 nonies dell'art. 64 l'accesso ai servizi in rete erogati dalle pubbliche amministrazioni, oltre che tramite il sistema SPID può sempre essere effettuato avvalendosi della carta di identità elettronica e della carta nazionale dei servizi.

Il comma 2 decies dell'art. 64 specifica che i gestori di identità digitale e degli attributi qualificati dovranno fornire gratuitamente alle pubbliche amministrazioni i propri servizi di verifica dell'identità, degli attributi non qualificati e di quelli qualificati.

Infine con il correttivo da ultimo approvato si è voluto specificare che le pubbliche amministrazioni dovranno utilizzare esclusivamente le identità digitali per l'identificazione degli utenti dei propri servizi on line a partire dalla data che sarà definita in un apposti decreto del Consiglio dei ministri o, in alternativa, con decreto del ministro per la semplificazione e la pubblica amministrazione.

2.8 Alfabetizzazione informatica dei cittadini

E' ovvio che l'obiettivo di un rapporto più diretto e veloce con le pubbliche amministrazioni per il tramite della sua progressiva digitalizzazione non potrebbe essere conseguito se i gli utenti non fossero in grado di utilizzare gli strumenti offerti dal digitale. Ed è proprio per tale ragione che il legislatore ha ritenuto necessario prevedere nell'art. 8 del CAD che lo Stato e le pubbliche amministrazioni siano tenute ad adoperarsi per la diffusione della cultura informatica tra i cittadini.

La previsione in oggetto specifica poi che si dovrà porre una particolare attenzione alla formazione dei minori e delle categorie a rischio di esclusione. A dire il vero non sembra che sia possibile ravvisare un deficit di competenze informatiche nei minori i quali, anzi, sempre più frequentemente definiti con l'espressione "nativi digitali", appaiono avere molta dimestichezza con gli strumenti informatici. Forse il legislatore avrebbe dovuto al contrario prevedere una particolare attenzione nella promozione della cultura informatica tra le fasce più anziane della popolazione (che in ogni caso è possibile includere nell'espressione "categorie a rischio di esclusione").

In che modo lo Stato e le pubbliche amministrazioni dovranno adempiere all'obbligo di promozione della cultura informatica? Lo prevede l'ultima parte dell'art. 8 ai sensi del quale dovranno essere intraprese azioni specifiche e concrete avvalendosi anche del servizio radiotelevisivo.

2.9 Il responsabile per la transizione digitale

Già il D.Lgs. 26 agosto 2016 n. 179 aveva previsto, all'art. 17, che, dovendo le pubbliche amministrazioni garantire <<l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo>>, ciascuna di esse ha il compito di affidare <<a un **unico ufficio dirigenziale generale**, fermo restando il numero complessivo di tali uffici, **la transizione alla modalità operativa digitale** e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Oggi, il nuovo correttivo mantiene questa figura, attribuendole nuova forza.

Innanzi tutto, la rubrica della norma è mutata da <<Strutture per l'organizzazione, l'innovazione e le tecnologie>>, a <<Responsabile per la transizione digitale e difensore civico digitale>>, con ciò volendo il legislatore delegato focalizzare tale ruolo, che può essere cruciale in questi anni che appaiono decisivi per la definitiva digitalizzazione della pubblica amministrazione italiana.

I **compiti** del responsabile per la transizione digitale sono specificamente elencati al comma 1 del medesimo art. 17, e tra questi sono degni di particolare menzione:

il coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

l'accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

l'analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonchè di ridurre i tempi e i costi dell'azione amministrativa;

la pianificazione ed il coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale.

Il correttivo 2018 ha inoltre introdotto un ulteriore compito, che incide sulle scelte da effettuare in sede di **acquisto di beni e servizi informatici**: <<pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale>> (art. 17 comma 1 lett. j-bis, CAD).

Quali sono i requisiti che deve possedere il soggetto a cui affidare tale ruolo? Il comma 1-sexies precisa che, nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato individuano l'ufficio tra quelli di **livello dirigenziale** oppure, ove ne siano privi, individuano un responsabile per il digitale tra le **proprie posizioni apicali**.

L'atto di nomina dovrà contenere, in ossequio all'autonomia organizzativa di ogni singolo ente pubblico, la specificazione di compiti ed attribuzioni, nonché l'indicazione dello staff che lo assisteranno in tale ruolo.

Il responsabile per la transizione al digitale risponde, con mero riferimento ai compiti relativi alla transizione, direttamente all'organo di vertice politico; in assenza di tale figura (ad es., i singoli istituti scolastici), il responsabile dell'ufficio per il digitale risponde direttamente a quello amministrativo dell'ente.

Un'ulteriore novità dettata dal correttivo 2018 è senza dubbio quella dettata dal nuovo comma 1-septies, secondo cui le pubbliche amministrazioni diverse dalle amministrazioni dello Stato <<possono esercitare le funzioni di cui al medesimo comma anche **in forma associata**>>: si tratta evidentemente di una novità molto interessante per gli enti locali, ed in generale per tutte le piccole amministrazioni, scuole comprese, che possono incontrare maggiori difficoltà, di tipo sia economico che di gestione del personale, nell'attribuire tale ruolo nell'ambito del proprio personale.

2.10 Formazione informatica dei dipendenti pubblici

La progressiva digitalizzazione della pubblica amministrazione non può non incidere anche sui sistemi di reclutamento e formazione del personale.

Già il precedente correttivo, all'art. 13, aveva sancito che le pubbliche amministrazioni devono attuare politiche di formazione del personale finalizzate alla **conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione**, e dei temi relativi all'accessibilità e alle tecnologie assistive ai sensi dell'articolo 8 della legge 9 gennaio 2004 n. 4; addirittura, tali politiche di formazione devono essere volte allo sviluppo delle competenze tecnologiche, di **informatica giuridica e manageriali dei dirigenti** per la transizione alla modalità operativa digitale.

Ed infatti, l'art. 17 comma 1-ter prevede che il responsabile per la transizione digitale debba essere necessariamente dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali.

Oggi, il nuovo correttivo compie un giro di vite, e stabilisce addirittura che la conoscenza e l'uso delle tecnologie dell'informazione e della comunicazione debbano essere tra le preminenti finalità **delle politiche di reclutamento**.

2.11 Il difensore civico digitale

Come anticipato, l'art. 17 è stato rubricato dal nuovo correttivo <<Responsabile per la transizione digitale e difensore civico digitale>>.

L'ultima stesura di tale articolo, al comma 1-quater, riscrive infatti completamente la figura del difensore civico digitale, istituito presso l'AgID, ed in possesso di adeguati requisiti di terzietà, autonomia e imparzialità.

Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, **segnalazioni relative a presunte violazioni del CAD** e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione commesse dalle pubbliche amministrazioni.

Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita l'amministrazione responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni, e la segnala all'ufficio competente per i procedimenti disciplinari interno all'amministrazione stessa.

Le decisioni del difensore civico sono pubblicate in un'apposita area del sito Internet istituzionale.

Capitolo 3
DOCUMENTI INFORMATICI E FIRME ELETTRONICHE

3.1 Documento informatico e firme elettroniche

Il Codice dell'Amministrazione Digitale definisce il documento informatico all'articolo 1, comma 1, lett. p), come: "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Per "atto", in diritto, si deve intendere un fatto consistente in un comportamento umano rilevante per l'ordinamento giuridico, poiché volontario. Elemento costitutivo è dunque l'imputazione a un soggetto di diritto, che può essere la persona fisica che ne ha voluto l'accadimento o la persona giuridica per la quale detta persona fisica ha agito in qualità di organo, nonché la volontarietà che, a sua volta, implica la consapevolezza da parte di chi ha agito, ossia la sua capacità di comprendere e, quindi, liberamente volere. Esempi sono da considerarsi il testamento, la sentenza, il contratto, l'atto amministrativo.

Per “fatto” si deve intendere un accadimento che avviene nella realtà materiale (“fatto naturalistico”) e non si concretizza in un comportamento umano. Se il fatto è considerato all’interno di una norma, allora il suo verificarsi diviene rilevante per l’ordinamento (“fatto giuridico”). E’ lecito affermare che tutti i fatti giuridici sono altresì fatti naturalistici, mentre non è vero il contrario. Un esempio di fatto giuridico è il decorso del tempo.

Per “dato” si deve intendere una descrizione elementare, spesso codificata, di un’entità, di un fenomeno, di una transazione, di un avvenimento o di altro. Nasce dall’osservazione di aspetti e fenomeni elementari; esso permette di effettuare dei calcoli, risolvere un problema, caratterizzare un fenomeno o esprimere un’opinione. Il dato può divenire “informazione” per un soggetto solo se comporta un reale aumento di conoscenza.

Tale definizione è il frutto delle evoluzioni che si sono a lungo susseguite in questa materia, a partire dal D.P.R. n. 531/1997, e costituisce il punto centrale attorno a cui ruota gran parte del Codice e che, da ultimo, è stato oggetto della incisiva azione della normativa europea, con il **Regolamento del Parlamento e del Consiglio del 23 luglio 2014 n. 910, cd. Regolamento eIDAS (electronic IDentification Authentication and Signature)**. Risulterebbe difficile, in effetti, poter parlare di Pubblica Amministrazione digitale senza che la parte più corposa e rilevante della sua attività (vale a dire la formazione, la trasmissione e la conservazione della documentazione amministrativa) sia realizzata in forma elettronica.

Sul punto occorre però precisare che **l’introduzione della locuzione “documento elettronico” nella definizione del C.A.D. di “documento informatico”** (presente nel nostro ordinamento sin dagli anni ‘90 del secolo scorso) è stata essenzialmente dovuta alla necessità di **assolvere al Regolamento eIDAS** che, appunto, non definisce i documenti informatici ma quelli elettronici. In futuro tale riferimento all’elettronica potrebbe perdere di necessità e vigore, data la possibile realizzazione di computer quantici (o quantistici), volti quindi ad utilizzare i quanti e non gli elettroni, come già da tempo preannunciato da Google: ciò porterà all’abbandono del documento elettronico in favore del documento quantico.

Al di là delle doverose puntualizzazioni sull’introduzione della locuzione “documento elettronico”, l’intero concetto di Amministrazione Digitale ruota di fatto intorno a quella che viene chiamata **“rappresentazione informatica”** e può essere definita non solo come il risultato della trasformazione in bit, e successiva memorizzazione su supporto informatico, di quegli atti, fatti o dati che possano avere rilevanza giuridica, ma anche come il contenuto elettronico vero e proprio, a prescindere da quale che sia la sua genesi.

Per cui “documento informatico” può essere **un file di testo, una foto, un video, un audio, che rappresenti informaticamente o conservi elettronicamente un atto, un fatto o un dato rilevanti giuridicamente.**

Il Regolamento eIDAS, infatti, dal canto suo, definisce “documento elettronico”, qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

Il C.A.D. dedica l’intero Capo II alla disciplina del documento informatico e delle firme elettroniche mentre il Regolamento eIDAS dedica il capo IV al documento elettronico e la sez. IV del capo III alle firme elettroniche (artt. 25-34)

Una volta stabilita la rilevanza giuridica del documento informatico-elettronico, è venuta meno la necessità di prevederlo espressamente.

La Sezione II del Capo II del C.A.D. è interamente dedicata alle firme elettroniche ed ai certificatori.

Volendo semplificare l’esposizione, per donare al lettore un facile quadro di riferimento, è possibile dire che il C.A.D. distingue due macro-categorie di firme:

1. **la firma elettronica (semplice**), definita nel Regolamento eIDAS (art. 3, comma 1, n. 10) come quei “dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare”;

2. **la firma elettronica avanzata (FEA)**, definita nel Regolamento eIDAS (art. 3, comma 1, n. 11) come “una firma elettronica che soddisfi i requisiti di cui all’articolo 26, ossia: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l’identificazione di ogni successiva modifica di tali dati”;

- **la firma elettronica qualificata (FEQ)**, definita nel Regolamento eIDAS (art. 3, comma 1, n. 12) come “una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche”;
- **la firma (qualificata) digitale**, definita nel C.A.D. (art. 1, comma 1, lett. s) come “un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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”.

Le firme elettroniche di un documento informatico, e in particolare le firme elettroniche avanzate e qualificate, tra cui quella digitale, si propongono di soddisfare tre esigenze che non tutte le tipologie di firma elettronica però soddisfano:

- che il destinatario possa verificare l'identità del mittente **(autenticità)**;
- che il mittente non possa disconoscere un documento da lui firmato **(non ripudio)**;
- che il destinatario non possa inventarsi o modificare un documento firmato da qualcun altro **(integrità)**.

Volendo ora procedere alla disamina delle singole tipologie di firma elettronica e partendo da quelle più basilari, sotto il profilo pratico la categoria delle firme elettroniche semplici può essere definita come una **categoria residuale**, nella quale confluiscono tutte le tipologie di firma che non detengono caratteri tali da configurarle come firme avanzate. Un classico esempio di scuola di firma elettronica semplice è quello della firma elettronica contenuta in una normale email: le credenziali di accesso riconosciute dal fornitore del servizio, infatti, integrano gli estremi di una firma elettronica semplice e, nella normalità dei casi, non di una firma avanzata.

L'art. 26 del Reg. eIDAS, a sua volta, stabilisce che una firma può essere considerata avanzata se:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Con il **Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 dal titolo "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali"** le firme avanzate hanno trovato una precisa regolamentazione tecnica nel nostro ordinamento, che produrrà i suoi effetti sino all'approvazione delle prossime Regole tecniche del C.A.D. (nella forma di Linee guida AgID, come da D.Lgs. n. 217/2017).

Come su evidenziato, all'interno della categoria delle firme elettroniche avanzate è possibile distinguere un altro gruppo di firme aventi caratteristiche di particolare importanza, ovvero le **"firme qualificate"**, definite tali in quanto rilasciate da un **certificatore accreditato presso l'Agenzia per l'Italia Digitale**. Nella realtà pratica, i certificatori accreditati sono soggetti pubblici o privati che emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).

Tra le firme qualificate, grande importanza occupa la **"firma digitale"**, la quale è un **particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche**, una **pubblica** e una

privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (differenziando per struttura le firme digitali, possiamo avere: CADES, apponibile a qualsiasi formato di file e ne modifica l'estensione rendendolo .p7m; PADES, apponibile solo sui file PDF e non modifica l'estensione; XADES, apponibile solo sui file XML e non modifica l'estensione). Quindi, le sue **caratteristiche tecniche più importanti** sono:

- la chiave pubblica (contenuta nel certificato qualificato);

- la chiave privata (custodita dal mittente).

In altre parole, il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra: da questa asimmetria nasce anche la definizione del meccanismo come "**crittografia asimmetrica**".

Affinché il sistema risulti sicuro, è necessario che solo l'utente che intende crittare il documento, e nessun altro, abbia accesso alla chiave privata: l'unica copia della chiave deve essere "in mano" all'utente, che deve impedirne l'accesso a terzi. Vi sono, però, soluzioni alternative, come l'uso di una "**firma digitale remota**", ovvero una tipologia di firma digitale, accessibile via Rete (Intranet e/o Internet), nella quale la chiave privata del firmatario viene conservata assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM - Hardware Security Module) da parte di un certificatore accreditato. Il firmatario viene identificato dal servizio e autorizza l'apposizione della firma tramite un meccanismo di sicurezza fra i quali:

- PIN firma di tipo statico, ovvero un codice numerico che consente l'uso di dispositivi elettronici solo a chi ne è a conoscenza;
- token OTP, ovvero un sistema che genera una password valida solo per una singola sessione di accesso o transazione;
- riconoscimento grafometrico della firma autografa;
- telefono cellulare (come OTP) seguito da PIN firma.

Il **meccanismo di firma digitale** è semplice, riassumibile nelle seguenti fasi:

a. l'utente, avviando lo strumento di firma digitale sul proprio computer, ricava innanzitutto **l'impronta digitale** del documento con l'ausilio di una **"funzione hash"** (pubblica), detta anche message digest: l'impronta digitale si concretizza in un file di dimensioni relativamente piccole (128, 160 o più bit), che contiene una sorta di codice di controllo relativo al documento stesso; la funzione hash è fatta in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta, inoltre, è one-way, a senso unico, questo significa che

dall'impronta è impossibile ottenere nuovamente il testo originario, quindi questa è "non invertibile";

b. l'utente utilizza, poi, la propria **chiave privata per cifrare l'impronta digitale**: il risultato di questa codifica è la firma; la firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente;

c. a questo punto **la firma viene allegata al documento** che si intende sottoscrivere, insieme alla chiave pubblica;

d. il destinatario del documento su cui è apposta una firma digitale può verificarne l'autenticità: per farlo, **decifra la firma del documento con la chiave pubblica del mittente**, ottenendo l'impronta digitale del documento, e quindi **confronta quest'ultima con quella che si ottiene applicando la funzione hash** al documento ricevuto; se le due impronte sono uguali, l'autenticità e l'integrità del documento sono garantite; si tratta, in realtà, di un'operazione sostanzialmente automatica svolta dal computer, quindi pressoché immediata e semplice da realizzare per il destinatario, previa installazione sul proprio device del software di verifica, scaricabile gratuitamente dal sito dell'Agenzia per l'Italia Digitale (AgID).

Nel loro uso combinato, dunque, le due chiavi servono a garantire e a verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La firma digitale rappresenta l'equivalente elettronico della tradizionale firma autografa su carta ed è univocamente associata al documento elettronico sul quale è apposta, attestandone con certezza, l'integrità, l'autenticità, la non ripudiabilità.

L'utilizzatore di firma elettronica qualificata o di firma (qualificata) digitale deve prestare particolare attenzione ai casi di scadenza temporale del proprio certificato di firma, di revoca o sospensione dello stesso. Infatti, l'apposizione di una firma digitale con **certificato scaduto, revocato o sospeso equivale a mancata sottoscrizione**. È ciò che stabilisce **l'art. 24 comma 4-bis** del C.A.D., prevedendo per la validità della sottoscrizione l'utilizzo di un certificato qualificato in corso di validità, attraverso il quale si possano rilevare gli elementi identificativi del titolare e del certificatore. Normalmente il certificato di firma digitale, rilasciato dall'ente certificatore, ha una durata biennale e o triennale.

Nel caso in cui il certificato di firma digitale sia scaduto, è necessario rivolgersi al proprio ente certificatore al fine di procedere al **rinnovo, oppure dotarsi di nuovo certificato** presso uno dei soggetti abilitati dall'Agenzia per l'Italia Digitale.

Revoca o sospensione del certificato hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che di essa ne erano già a conoscenza tutte le parti interessate.

Per quanto attiene alla validità nel tempo di firme qualificate o digitali il cui certificato sia scaduto, revocato o sospeso, in base all'art. 62, comma 1, delle citate Regole tecniche del 2013 sulle firme avanzate **sono comunque da ritenersi valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato**. Detto in altre parole, gli odierni sistemi di firma digitale evidenziano, nella loro normalità, il campo signing time (momento della firma), inserendo in automatico data e ora di sottoscrizione nella busta crittografica della firma qualificata o digitale: tale indicazione di data e ora può essere ritenuta un riferimento temporale, considerando quest'ultimo come "l'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento" (Regole tecniche sul documento informatico – DPCM 13 novembre 2014). Riassumendo, **se il riferimento temporale generato dal meccanismo di firma qualificata o digitale è anteriore alla data e ora di scadenza, revoca o sospensione del certificato allora la firma detiene comunque validità nel tempo**.

Tra gli altri processi comunemente in grado di attribuire un riferimento temporale occorre citare, in base all'art. 41 del DPCM 22 febbraio 2013: le marche temporali, la segnatura del protocollo informatico, la conservazione digitale o l'utilizzo di PEC.

Una volta descritto il quadro delle firme elettroniche, anche nell'ottica comparativa con le firme analogiche, possiamo passare a descrivere le diverse ipotesi che si possono incontrare in base al tipo di firma elettronica apposta al documento informatico.

Occorre distinguere due situazioni tra loro differenti, ossia:

- **l'efficacia probatoria** del documento informatico;
- la sua capacità di soddisfare il **requisito della forma scritta**.

3.2 Efficacia probatoria e requisito della forma scritta

Per quanto riguarda **l'efficacia probatoria** del documento informatico, essa è da intendersi come **la "forza" che determinati documenti hanno come prova di un fatto una volta assunti in un processo**; pertanto, è la capacità di quei determinati atti di provare il loro contenuto.

Volendo ora affrontare la questione del **requisito della forma scritta** di un documento, primariamente occorre sottolineare come la rappresentazione di un atto, fatto o dato può avere diverse forme (modalità di rappresentazione): scritta, orale, attraverso segnali ottici o sonori, ed altre ancora. La forma scritta, pertanto, è solo una delle possibili, visto il **principio di libertà delle forme** previsto nel nostro ordinamento, ma detiene una valenza fondamentale, perché solo ad essa,

e quindi per esemplificare non ad un documento orale, è possibile riconoscere un particolare valore in determinate circostanze.

La forma scritta è posta soprattutto a tutela di una o di entrambe le parti in un rapporto negoziale (come un contratto), poiché serve ad attirare l'attenzione dei contraenti rispetto all'atto che stanno per compiere ed alla sua importanza. Inoltre, con l'atto scritto si certifica la volontà delle parti e si agevola la prova della sua esistenza.

Normalmente la forma scritta si riconduce nel nostro ordinamento a due concetti:

a) forma scritta **ad substantiam** ("ai fini della sostanza"), richiesta per l'**esistenza** stessa del negozio (come per es. per un contratto di compravendita di una casa);

b) forma scritta **ad probationem** ("ai fini della prova"), richiesta solo per **provare l'esistenza** del negozio giuridico (come per es. per un contratto di agenzia): nella generalità dei casi, un negozio giuridico può essere provato in giudizio mediante qualsiasi mezzo (ad es. mediante testimoni), accade però, che, in talune ipotesi, la legge, con disposizioni espresse, stabilisca che possa esser provato in giudizio solo mediante documenti, ossia per mezzo di atti aventi forma scritta; è necessario sottolineare che il negozio mancante della forma ad probationem è perfettamente valido ed efficace, ma, in caso di processo, l'unico modo per provare l'esistenza di quel particolare negozio sarà la forma che la legge richiedeva, salva la possibilità di ottenere una **confessione** (disciplinata dagli artt. 2730 e 2735 c.c..) o un **giuramento** (disciplinato dall'art. 2739 c.c..) in giudizio.

I privati possono convenzionalmente prevedere per i loro atti determinate forme, come nel caso in cui si stabilisca che la disdetta del contratto debba necessariamente avvenire per iscritto attraverso un telegramma; anche in questo caso è da ritenersi, salvo diversa volontà, che il mancato rispetto della forma prevista convenzionalmente comporti la nullità dell'atto.

Compresi i concetti di efficacia probatoria e requisito della forma scritta, occorre ora soffermarsi su quanto disciplinato a riguardo dal C.A.D. novellato con il D.Lgs. 217/2017.

In base all'art. 20, comma 1-bis, del C.A.D.: "Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di

formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".

Sotto il profilo dell'efficacia probatoria, il comma fa riferimento a quella prevista dall'art. 2702 del Codice Civile per la **scrittura privata** (alla quale, quindi, il documento informatico con firma digitale, elettronica qualificata, elettronica avanzata o identificazione informatica del suo autore è parificato ai fini probatori): in base all'art. 2702 c.c. **la scrittura privata** (quindi il semplice atto redatto tra le parti senza particolari formalità) fa **piena prova, fino a querela di falso,** della provenienza delle dichiarazioni da chi l'ha sottoscritta:

- se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione;

- ovvero se questa è legalmente considerata come riconosciuta.

Circa l'esposta portata probatoria del documento informatico, si rende necessaria una riflessione.

Il Legislatore aggiunge poi che: "L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria".

Ciò significa che nel momento in cui un soggetto adopera un dispositivo di firma elettronica qualificata o digitale deve sempre prestare il massimo dell'attenzione: infatti, l'uso indebito del dispositivo da parte di un altro soggetto porrebbe il titolare in una posizione processualmente scomoda, in quanto sarebbe costretto a fornire lui la prova di essere stato spogliato del possesso del dispositivo.

Altra novità del 2017, il nuovo comma 1-quater dell'art. 20 in esame che fa salva, comunque, la specialità della normativa, anche regolamentare, oggi esistente in tema di deposito degli atti e dei documenti in via telematica in materia di processo telematico

3.3 Copie di documenti e duplicati

Come detto, in genere, i documenti possono essere sia analogici che informatici.

Per entrambi, comunque, si pone il problema della circolazione del documento, che normalmente esiste anzitutto nella sua versione "originale".

Tuttavia, il documento originale può essere fatto circolare non direttamente, ma attraverso delle sue copie, appositamente realizzate.

Per quanto riguarda le varie ipotesi rinvenibili nel C.A.D., troviamo:

1) la **copia informatica di documento analogico** (ad esempio il caso di un documento originariamente cartaceo e il cui contenuto viene riportato interamente in bit o mediante l'utilizzo di strumenti OCR), definita dall'art. 1, comma 1, lettera i-bis, come "il documento informatico avente

contenuto identico a quello del documento analogico da cui è tratto"; l'art. 22, comma 1, del C.A.D. stabilisce il valore legale di atti pubblici, scritture private o documenti in genere, ivi compresi gli atti e documenti amministrativi, originariamente su supporto analogico e poi rilasciati con copia informatica da un pubblico ufficiale o altro soggetto autorizzato, come un notaio, attribuendo loro **efficacia** (ai sensi degli artt. 2714 e 2715 c.c.), quando sia apposta la **firma digitale, altra firma elettronica qualificata, firma elettronica avanzata o previa identificazione informatica del suo autore (attraverso un processo avente i requisiti fissati dall'AgID con Linee guida) da parte del soggetto che le ha rilasciate, volta ad attestarne la conformità all'originale**; le copie così create **sostituiscono gli originali analogici ad ogni effetto di legge**, anche sotto il profilo dell'esibizione e produzione in giudizio e l'assoluzione degli obblighi di conservazione;

2) la **copia per immagine su supporto informatico di documento analogico** (ad esempio la scansione di un documento originariamente cartaceo o la fotografia digitale dello stesso), definita dall'art. 1, comma 1, lettera i-ter, come "il documento informatico avente **contenuto e forma identici** a quelli del documento analogico da cui è tratto"; l'art. 22, comma 1-bis e 2, del C.A.D. dispone che la copia per immagine su supporto informatico di un documento analogico debba essere prodotta mediante processi e strumenti in grado di assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia; tali copie hanno la stessa efficacia probatoria degli originali da cui sono tratte, se la loro **conformità all'originale** è attestata da un notaio o altro pubblico ufficiale autorizzato (come un funzionario), nel rispetto delle regole tecniche (future Linee guida AgID);

3) la **copia (o estratto) informatica di documento informatico** (ad esempio quando si genera copia di un file passando da un estensione .doc a una .pdf), definita dall'art. 1, comma 1, lettera i-quater, come "il documento informatico avente **contenuto identico** a quello del documento da cui è tratto su supporto informatico **con diversa sequenza di valori binari**"; l'art. 23-bis, comma 2, del C.A.D. dispone che tali copie hanno il medesimo valore giuridico dei documenti informatici da cui sono tratte, se prodotte in conformità alle regole tecniche (future Linee Guida AgID) e la loro **conformità all'originale** è attestata da un pubblico ufficiale autorizzato o se la loro conformità **non è espressamente disconosciuta**; in tali casi, se previsto, resta fermo l'obbligo di conservazione del documento originale informatico;

4) la **copia analogica di un documento informatico** (ad esempio, la stampa di un file gestito e conservato dall'Amministrazione); l'art. 23 del C.A.D. dispone che tali copie hanno la stessa

efficacia probatoria dell'originale da cui sono tratte se la **conformità all'originale** è attestata da un pubblico ufficiale autorizzato oppure se il documento informatico originale è conforme alle regole tecniche (future Linee Guida AgID) e la conformità all'originale **non sia disconosciuta**; in tali casi, se previsto, resta fermo l'obbligo di conservazione del documento originale informatico.

Altra figura, distinta rispetto alla copia, e peculiare per il documento informatico, è il cd. **duplicato informatico**, ossia il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della **medesima sequenza di valori binari del documento originario: si tratta quindi del caso in cui si genera la versione di un file mantenendo la stessa estensione (da un .pdf ad un .pdf).**

Il duplicato informatico, per espressa disposizione dell'art. 23-bis del C.A.D., ha il **medesimo valore giuridico**, ad ogni effetto di legge, **del documento informatico da cui è tratto**, se prodotto in conformità alle regole tecniche di cui all'articolo 71 (future Linee Guida AgID).

Le norme ora esposte in tema di copie e duplicati si applicano anche all'attività della Pubblica Amministrazione. Due possono essere i classici casi in un'Amministrazione, che di seguito richiamiamo applicando la normativa già enucleata.

Un primo caso può essere quello della richiesta di un cittadino di copia analogica di un documento originariamente informatico dell'Amministrazione.

In base al citato art. 23 C.A.D. si deve provvedere per mezzo del soggetto incaricato (che in tal caso svolge la funzione di pubblico ufficiale) alla **stampa del documento originario informatico e all'attestazione di conformità** all'originale informatico del documento stampato, quindi apponendo il relativo timbro e firma. In questo modo la stampa di un documento originale informatico avrà la stessa efficacia del documento da cui è tratta.

Al fine di garantire la provenienza e conformità dell'atto alla sua versione originale, sulle copie analogiche dei documenti informatici che l'Amministrazione rilascia al cittadino è possibile apporre un **timbro digitale**, se l'applicativo lo consenta. Si tratta di un codice a barre bidimensionale (glifo), disciplinato dall'art. 23, comma 2-bis: "Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con Linee Guida, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I soggetti che procedono all'apposizione del contrassegno rendono disponibili gratuitamente sul proprio sito Internet istituzionale idonee soluzioni per la verifica del contrassegno medesimo". In altre parole, con la stampa di un documento amministrativo informatico è possibile l'apposizione

automatica di un timbro digitale, tale da non necessitare la copia creata di una dichiarazione di conformità firmata dal Pubblico Ufficiale. Il Timbro digitale, ove previsto negli applicativi, permette quindi di snellire notevolmente la fase di creazione di copie conformi analogiche derivanti da un file.

Altro classico caso che si verifica nelle Amministrazioni è la **ricezione di documenti cartacei, di cui si rende poi necessaria la scansione e acquisizione della relativa copia per immagine**. In particolare, al fine di garantire al documento informatico così ottenuto la stessa efficacia del corrispettivo analogico è necessario che il soggetto incaricato (secondo quanto previsto dall'art. 22 del C.A.D.) vi apponga una firma digitale.

Come rilevato da tutta l'analisi effettuata, le riproduzioni di un documento informatico possono avere la medesima portata probatoria degli originali da cui sono tratti: perché identiche, nel caso dei duplicati informatici, o perché dichiarate conformi da un pubblico ufficiale, nel caso delle copie informatiche o analogiche. È giusto affermare, quindi, che si tratti di una "**capacità probatoria dipendente**", poiché "la portata oggettiva della riproduzione è condizionata dall'attitudine probatoria dell'originale riprodotto"(FRANCHINI, MINAZZI).

3.4 Documento amministrativo informatico

L'art. 22, comma 1, lett. d), della Legge n. 241/1990 dal titolo "Nuove norme sul procedimento amministrativo", come novellato nel 2005, così definisce il documento amministrativo: "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

Pertanto, documento amministrativo può essere considerato una rappresentazione informatica di atti, anche interni, formati o utilizzati dalla Pubblica Amministrazione. Detto in altre parole, il "documento amministrativo informatico" si configura come species del genus "documento amministrativo".

L'art. 23-ter del C.A.D. ha poi disciplinato gli atti formati dalle Pubbliche Amministrazioni mediante strumenti informatici.

In base alla norma, gli atti formati dalle Pubbliche Amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Sempre secondo il C.A.D., art. 40: “Le Pubbliche Amministrazioni **formano gli originali dei propri documenti**, inclusi quelli inerenti ad albi, elenchi e pubblici registri, **con mezzi informatici** secondo le disposizioni di cui al presente codice e le Linee Guida”.

Il **DPCM 21 marzo 2013**, voluto dallo stesso C.A.D., ha poi elencato i (pochi) casi di “documento originale analogico unico”, ovvero quei casi nei quali l’originale dell’atto deve necessariamente rimanere cartaceo e la cui conservazione digitale è esclusa: tutti casi, quelli elencati dal DPCM, che comunque non impattano sul normale agere della generalità delle Amministrazioni (tra questi troviamo, a titolo di esempio, gli atti giudiziari, processuali o di polizia giudiziaria e gli atti notarili), confermando la regola generale, di cui all’art. 40, in base alla quale la “forma informatica” costituisce un obbligo generale.

Va sottolineato che formare gli originali significa non solo **redigere** il testo con l’ausilio degli strumenti informatici, ma anche **sottoscrivere** gli atti in modalità elettronica. Pertanto, l’art. 40 non attribuisce alle Amministrazioni un potenziale strumento per operare, il documento informatico, ma ne prescrive la totale e assoluta obbligatorietà, da ciò derivando una **nullità di eventuali atti amministrativi nel momento in cui non rispettino la forma informatica**. Il procedimento logico giuridico che conduce alla nullità deriva dal combinato dell’art. 40 C.A.D. e dell’art. 21-septies della Legge n. 241/1990 che prescrive: “È nullo il provvedimento amministrativo che **manca degli elementi essenziali**, che è viziato da difetto assoluto di attribuzione, che è stato adottato in violazione o elusione del giudicato, nonché negli altri casi espressamente previsti dalla legge”.

Per dottrina (PERONGINI) e giurisprudenza (Cons. Stato, Sezione VI, 14 luglio 1999, n. 948), **tra gli elementi essenziali, la cui mancanza comporta la nullità dell’atto, rientra anche la “forma”**, come quella informatica prescritta per tutti i documenti amministrativi dall’art. 40 C.A.D.. La mancanza di tale forma informatica, dunque, comporta la nullità dell’atto. Con particolare riferimento alla forma, infine, occorre precisare che non ogni carenza formale dell'atto porta alla nullità dello stesso: l'art. 21-octies della Legge n. 241/1990, infatti, esclude la “violazione di norme sulla forma degli atti” dallo stesso ambito dell'annullabilità, degradando il vizio relativo a mera irregolarità, almeno quando esso riguardi provvedimenti contenutisticamente vincolati. Pertanto, si avrà nullità del provvedimento amministrativo solo in mancanza della forma essenziale, intendendosi per forma essenziale l'insieme delle caratteristiche esteriori necessarie e sufficienti ad identificare un atto come proveniente da una Pubblica Amministrazione., oltre a renderne intelligibile il dispositivo. A parere di chi scrive, per forma essenziale è assolutamente lecito ritenere la “forma informatica” come prescritta dall’art. 40 C.A.D., posizione avvalorata dalla stessa semantica rigorosa e scevra da qualsivoglia possibile fraintendimento utilizzata dal Legislatore nella

norma. In ogni caso, al momento in cui si scrive non vi sono arresti giurisprudenziali che abbiano preso una posizione definita a riguardo.

Da ultimo, del documento amministrativo informatico si è interessato il DPCM 13 novembre 2014, oggi ancora in vigore, contenente le "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle Pubbliche Amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005".

Le regole tecniche dedicano il capo III alla disciplina del documento amministrativo informatico che presenta specifiche peculiarità rispetto al documento informatico disciplinato nei capi precedenti.

Nella formazione dei documenti amministrativi, difatti, assumono una particolare rilevanza:

a) **l'uso degli strumenti riportati nel manuale di gestione documentale** di ciascuna Amministrazione;

b) **l'acquisizione delle istanze, dichiarazioni e comunicazioni** di cui agli articoli 5-bis (comunicazioni tra imprese e Amministrazioni), 40-bis (protocollo informatico) e 65 (istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica) del C.A.D..

In altre parole, **in base alle regole tecniche i casi ora elencati alle lettere a) e b) generano documenti amministrativi informatici.**

Particolarmente importante è la specificazione secondo la quale il documento amministrativo informatico assume le caratteristiche di **immodificabilità e di integrità** anche con la sua semplice **registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti**, come richiesto dalla normativa di settore.

Ai fini della trasmissione telematica di documenti amministrativi informatici, le Pubbliche Amministrazioni pubblicano sui loro siti gli standard tecnici di riferimento, le codifiche utilizzate e le specifiche per lo sviluppo degli applicativi software di colloquio, rendendo eventualmente disponibile gratuitamente sul proprio sito il software per la trasmissione di dati coerenti alle suddette codifiche e specifiche.

Un interessante ambito di discussione dottrinaria (MASUCCI, DUNI, MARONGIU, COSTANTINO) è rappresentato da quello in tema di **"atto amministrativo automatizzato"**, ovvero la possibilità, o meno, degli odierni sistemi informatici di porre in essere atti, in toto o in parte, senza l'ausilio umano ma solo tramite l'elaborazione automatica dei dati inseriti sulla base delle istruzioni contenute nel software. Secondo alcuni sarebbe possibile e auspicabile giungere ad una totale

automatizzazione di talune categorie provvedimentali. Ma la più attenta dottrina ha rilevato come, in realtà, anche in casi vincolati di azione amministrativa, dove l'esercizio del potere pubblico non può uscire da binari rigidi preventivamente tracciati dal Legislatore, la discrezionalità amministrativa è spesso solo latente e, in talune circostanze, risorge, minando alla base la sequenzialità logica di un possibile software di automatizzazione. Il problema è aperto ma, a parere di chi scrive, difficilmente troverà compimento nel prossimo futuro, visto che il carattere essenziale del diritto amministrativo è quello di trovare soluzioni contemperando di volta in volta interessi diversi, pubblici e privati, contemperazione che, in questa fase storica, non è gestibile tramite l'elaborazione automatica di un algoritmo.

3.5 Atto pubblico e nullità

Per **atto pubblico** occorre intendere, in base all'art. 2699 del Codice Civile: "Un atto scritto, redatto interamente dal notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato".

Per **pubblico ufficiale**, in base all'art. 357 del Codice Penale, bisogna intendere chi esercita, anche temporaneamente, una funzione legislativa, amministrativa o giudiziaria con o senza rapporto di impiego con lo Stato o altro ente pubblico.

Secondo la dottrina e la giurisprudenza, però, la nozione penalistica di atto pubblico è più ampia di quella civilistica comprendendo, oltre ai documenti contemplati dall'art. 2699 c.c., **tutti quelli formati da un pubblico ufficiale o da un pubblico impiegato incaricato di pubblico servizio e compilati, con le prescritte formalità, per uno scopo di diritto pubblico**, inerente all'esercizio della propria funzione o del pubblico servizio, al fine di comprovare un fatto giuridico o di attestare fatti da lui compiuti o avvenuti in sua presenza ed aventi rilevanza giuridica. In definitiva, **nel concetto penalistico di atto pubblico, particolarmente ampio,** rientrano:

- tutti gli atti pubblici di cui all'art. 2699 del Codice civile;
- qualsiasi documento interno di un pubblico ufficio che possa assumere carattere probatorio e rilevanza esterna ai fini della documentazione di fatti inerenti all'attività dell'ufficio cui è addetto l'autore e la regolarità delle sue operazioni amministrative (ad esempio, sono stati considerati atti pubblici i registri di protocollo e i fogli di raccolta delle firme di presenza dei dipendenti pubblici);
- qualsiasi documento che costituisca corrispondenza ufficiale di organi della pubblica amministrazione;
- qualsiasi documento redatto da un pubblico impiegato incaricato di un pubblico servizio nell'esercizio delle sue attribuzioni.

L’interpretazione penalistica è quella maggiormente accolta in dottrina, se non altro perché i profili di responsabilità penale sono i più delicati per un Pubblico Ufficiale o incaricato di pubblico servizio, ragione legittimante la loro condivisione nell’interpretazione degli istituti giuridici.
Da ciò consegue che, ad esempio, in un Comune le delibere di Giunta, di Consiglio, le determine dirigenziali o gli atti di liquidazione sono da considerarsi “atti pubblici”.
Compresa la definizione civilistica e penalistica di “atto pubblico”, occorre ora **verificare se il nostro ordinamento richiede una forma specifica a pena di invalidità.**
Nello specifico, ex **art. 21 co. 2-ter C.A.D.**: “Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110 [atto pubblico informatico redatto dal notaio], **ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale**. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti”.
Da quanto detto, gli atti pubblici **necessitano di una firma qualificata o digitale a pena di nullità ai sensi dell’art. 21 co. 2-ter C.A.D. su indicato e non di una semplice firma elettronica avanzata** (men che meno di una firma elettronica semplice).

3.6 Procedimento amministrativo informatico

Dato l’impianto normativo su esplicato, il documento amministrativo informatico trova oggi una sua puntuale disciplina. Per il procedimento amministrativo informatico la situazione è più complessa.
Il “procedimento amministrativo”, in senso lato, è da intendersi come una **sequenza di atti amministrativi che portano all’emanazione di un atto finale (il provvedimento)**, e che quindi concorrono al conseguimento di un interesse pubblico. Pertanto, il procedimento amministrativo rappresenta la forma esteriore attraverso la quale si dispiega l’azione amministrativa, ovvero quel particolare iter procedurale che rende l’atto efficace e perfetto, nel pieno rispetto dell’art. 97 della nostra Costituzione e della disciplina primaria di settore dettata dalla Legge n. 241/1990.
Compreso il concetto di “procedimento amministrativo” è giusto ora sottolineare come non esista una definizione normativa di “procedimento amministrativo informatico”, né tantomeno una sua puntuale disciplina all’interno di un unico testo legislativo.
Infatti, la Legge n. 241/1990 sul procedimento amministrativo è stata ideata e scritta con obiettivi essenzialmente “analogici” (si pensi che non era ancora nata Internet come oggi la intendiamo), poi nel tempo integrata sempre più in senso “digitale”. Si veda, ad esempio, l’art. 3-bis, introdotto con

la Legge n. 15/2005, secondo il quale la Pubblica Amministrazione, per conseguire maggiore efficienza nella sua attività, deve incentivare l'uso della telematica, nei rapporti interni, tra le diverse Amministrazioni e tra queste e i privati. Ma, a parere di chi scrive, l'impianto di fondo della Legge n. 241/1990 rimane comunque "analogico", motivo per il quale autorevole dottrina ha giustamente sottolineato come il modello del "procedimento sequenziale" di tale legge, quindi ripartito per rigide fasi, sia in realtà in fase di totale superamento a causa del processo di informatizzazione pubblico, con un **passaggio al "procedimento a stella"**: "il concetto di procedimento a stella, alternativo al classico procedimento sequenziale, non è un'invenzione o una proposta dottrinale, ma una constatazione, derivante dalla scomparsa del fascicolo cartaceo che imponeva una sequenzialità legata alla necessità di disporre della documentazione cartacea per ogni intervento. La disponibilità in Rete del fascicolo informatico, contenente tutti gli elementi, consente di compiere le attività necessarie contemporaneamente, salvo il caso di diversa prescrizione legislativa o di palese inopportunità"(DUNI). Da questa riflessione scaturisce la convinzione di un progressivo "impoverimento applicativo" della Legge n. 241/1990: ancora vigente, ma che prosegue il suo cammino lungo modelli procedimentali inadatti alla realtà digitale e, nella sua disciplina del diritto di accesso documentale, già superata dal nuovo diritto di accesso generalizzato di cui al D.Lgs. n. 33/2013, di cui appresso meglio si dirà.

Lo stesso Consiglio di Stato, con i rilievi allo schema del C.A.D. svolti dalla sezione consultiva per gli atti normativi (Adunanza del 7 febbraio 2005), richiamava l'attenzione del Legislatore sulla necessità di una "perimetrazione" del Codice con riferimento alla disciplina del procedimento amministrativo. Richiamo non considerato appieno dal Legislatore nel testo finale del C.A.D..

Ad oggi, quindi, una disciplina unica e puntuale sul procedimento amministrativo informatico, contenuta in un unico testo legislativo e al passo con una visione procedimentale a stella, non esiste. È fondata, comunque, la posizione in dottrina secondo la quale, in base alla normativa vigente (essenzialmente C.A.D. e DPR n. 445/2000), sia possibile oggi espletare e gestire il procedimento amministrativo esclusivamente in forma elettronica (MASUCCI). L'interprete, dunque, può oggi ricostruire una **disciplina compiuta del procedimento amministrativo informatico, ma sempre da una sommatoria di norme contenute in diversi testi normativi di settore**. Il C.A.D., probabilmente, poteva essere il luogo ideale ove ricostruire un'unica disciplina sul procedimento amministrativo informatico o, comunque, è auspicabile possa divenirlo in futuro.

Delle norme di interesse in tema di procedimento amministrativo e Web sono anche contenute nel cd. Decreto Trasparenza, ovvero il D.Lgs. n. 33/2013. Il suo art. 35, c. 1, lett. d) dispone che le Amministrazioni pubblichino nella sezione "Amministrazione trasparente", sotto-sezione di primo livello "Attività e procedimenti", sotto-sezione di secondo livello "Tipologie di procedimento", gli

atti e i documenti da allegare alle istanze, oltre che la modulistica necessaria, compresi i fac-simile per le autocertificazioni.

Nella pubblicazione della modulistica sui siti istituzionali è innanzitutto necessario rispettare le disposizioni previste dalla citata L. n. 4/2004 in tema di accessibilità. Pertanto, i moduli pubblicati dovranno essere dei file accessibili. Una specifica accortezza, non richiesta dalla norma e quindi di rado considerata dalle Amministrazioni, è quella di pubblicare file editabili e salvabili, al fine di ridurre la mole di documenti cartacei in entrata.

3.7 Fascicolo informatico e Sistema pubblico di ricerca documentale

Come già evidenziato, le Pubbliche Amministrazioni sono del tutto obbligate a formare gli originali dei propri atti come documenti informatici (art. 40, comma 1, D.Lgs. n. 82/2005), nel rispetto delle disposizioni del C.A.D. e delle relative regole tecniche. Quindi, ogni documento amministrativo deve non solo nascere informaticamente ma anche essere gestito con le stesse modalità: l'**art. 41**, infatti, dispone che per la gestione amministrativa dei documenti occorre utilizzare le tecnologie dell'informazione e della comunicazione e, più nello specifico, occorre **raccogliere in un fascicolo informatico gli atti, i documenti e i dati di ogni procedimento amministrativo, da chiunque formati**.

Di conseguenza, l'unico fascicolo che l'ufficio deve creare è quello informatico avendo cura di inserire nello stesso sia i documenti digitali (ricevuti da privati-altre Amministrazioni o formati dall'Amministrazione) sia i documenti analogici acquisiti al sistema informatico (ad es., tramite scansione).

Il fascicolo informatico deve essere realizzato garantendo la possibilità di essere **direttamente consultato ed alimentato da tutte le Amministrazioni coinvolte nel procedimento**. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo devono essere 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 ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa.

In base al **comma 2-ter dell'art. 41** del C.A.D., il fascicolo informatico deve recare l'indicazione:

- dell'Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre Amministrazioni partecipanti;

- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il Sistema pubblico di ricerca documentale (di cui meglio appresso si dirà) nel rispetto delle Linee Guida AgID.

Il fascicolo informatico può contenere aree a cui hanno accesso solo l'Amministrazione titolare e gli altri soggetti da essa individuati. Esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata Legge n. 241/1990, in primis quelli di accesso ai documenti.

Il fascicolo informatico deve essere sempre realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le Amministrazioni coinvolte nel procedimento e dagli interessati, nei limiti ed alle condizioni previste dalla disciplina vigente, attraverso il Sistema pubblico di accesso documentale (art. 40-ter) e il Punto di accesso telematico dei servizi in rete delle Amministrazioni, attivato presso la Presidenza del Consiglio dei Ministri (art. 64-bis).

Normalmente, nelle Amministrazioni sono utilizzate le seguenti tipologie di fascicolo (PENZO DORIA):

- **per procedimento amministrativo**, nel momento in cui occorra conservare una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale;
- **per affare**, nel momento in cui occorra conservare i documenti relativi ad una competenza generalmente non proceduralizzata, per la quale, dunque, non è prevista l'adozione di un provvedimento finale, inteso come atto dotato di capacità di incidere nella sfera giuridica di terzi;
- **per attività**, nel momento in cui occorra conservare i documenti relativi ad una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale (la differenza essenziale con il fascicolo di affare è che mentre quest'ultimo conserva in modo organico documenti relativi a un medesimo argomento e di norma non prende avvio con un'istanza di parte, il fascicolo di attività conserva documenti relativi ad argomenti diversi pressoché privi di organicità);

- **per persona**, fisica o giuridica, nel momento in cui occorra conservare documenti relativi a diversi procedimenti amministrativi, distinti affari o diverse attività, ma legati da un vincolo archivistico interno, relativo ad una persona (fisica o giuridica che sia).

Volendo ora chiarire la portata del Sistema pubblico di ricerca documentale, esso è da intendersi come un sistema promosso dalla Presidenza del Consiglio dei Ministri e volto a facilitare la ricerca da parte di cittadini e imprese dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo e dei fascicoli dei procedimenti, nonché a consentirne l'accesso on-line ai soggetti che ne abbiano diritto ai sensi della disciplina vigente (art. 40-ter).

Tale componente dovrebbe costituire una sovrastruttura di livello nazionale in grado di dialogare con i singoli sistemi delle Amministrazioni attraverso standard di interoperabilità con l'obiettivo di consentire, a soggetti autorizzati, il reperimento generalizzato di documenti e fascicoli procedimentali, ovunque prodotti.

3.8 Carta di identità elettronica e carta nazionale dei servizi

Ad oggi, il nostro Legislatore affronta il tema dell'identificazione elettronica sotto i diversi aspetti in cui esso si declina: carte elettroniche, sistema per l'identità digitale (SPID) e anagrafe nazionale della popolazione residente (ANPR).

Tralasciando l'esame delle cosiddette "identità digitali deboli", utilizzate dagli operatori online per l'accesso a servizi digitali (email, social media, eCommerce) costituite, di norma, da nome utente e password, oltre a una serie di attributi funzionali alla fruizione del servizio, le quali non hanno una valenza univoca in un procedimento civile o penale, il C.A.D. si occupa delle diverse misure di identificazione digitale definite "forti".

Per quel che riguarda le **carte elettroniche,** il C.A.D. (sia nella vecchia che nella nuova versione) distingue due tipologie, delle quali dà una definizione all'art. 1, precisando:

- alla lettera c) cosa debba intendersi per **"carta d'identità elettronica"**(CIE), ovvero "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";
- alla lettera d) la **"carta nazionale dei servizi"**(CNS), ovvero " il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle Pubbliche Amministrazioni".

La disciplina applicativa di tali strumenti è poi contenuta negli artt. 64 e seguenti del suddetto Codice, recentemente oggetto di intervento riformatore, ove vengono specificate le caratteristiche

tecniche che le carte elettroniche devono possedere e la funzione peculiare delle stesse. In particolare, è bene sin da subito chiarire che prima della novella del 2016 la CIE e la CNS costituivano gli strumenti cardine previsti dal Legislatore per consentire l'accesso dei cittadini ai servizi erogati in Rete dalle Pubbliche Amministrazioni, con specifica delimitazione alle attività per le quali era richiesta l'autenticazione informatica; oggi ad esse è stato affiancato, e reso preminente, lo SPID, il quale costituisce, insieme alle carte elettroniche, l'unico sistema di accesso ai servizi in Rete erogati da una Pubblica Amministrazione.

Pur essendo fortemente assimilabili, l'elemento discretivo che rende le citate carte elettroniche non sovrapponibili è dato dalla maggiore sicurezza garantita dalla CIE rispetto alla CNS: invero, la seconda non possiede alcune caratteristiche tecniche possedute dalla prima, come per esempio la foto del soggetto, la banda ottica, gli ologrammi di sicurezza, etc., che fanno sì da una parte che la CNS dia meno garanzie sull'identificazione del suo possessore, ma che, per converso, permettono una più agevole distribuzione dello strumento, indipendentemente dai canali istituzionali abilitati a rilasciare la CIE.

Se la CIE ha la funzione principale di sostituire il classico documento di riconoscimento cartaceo, utilizzando la CNS, inserita in un apposito lettore collegato ad un PC, si può fruire di numerosi servizi messi a disposizione dalle PA, quali la firma digitale, la tessera sanitaria, il codice fiscale, i pagamenti online, semplicemente accedendo da remoto agli uffici pubblici in Rete, in qualunque posto del territorio nazionale ci si trovi.

Non tragga in inganno la definizione della carta d'identità elettronica come documento per l'identificazione "**fisica**" del titolare.

Infatti, come appare evidente nella Sezione III del Capo V del C.A.D., intitolato "Identità digitali, istanze e servizi on-line", tanto la carta nazionale dei servizi quanto la carta di identità elettronica, insieme a SPID, costituiscono strumenti per l'accesso ai servizi erogati in Rete dalle Pubbliche Amministrazioni per i quali sia necessaria "l'identificazione **informatica**" (art. 64, comma 2-nonies, in particolare).

Con tale disposizione il Legislatore ha voluto chiaramente definire le suddette carte elettroniche come strumento forte per l'affermazione dell'identità digitale, codificando espressamente il loro utilizzo per poter ricevere i servizi delle Pubbliche Amministrazioni in un'ottica di informatizzazione amministrativa completamente equivalente al modello fisico/cartaceo.

Da ultimo è bene dare atto che, se ad oggi il cittadino italiano ha ancora facoltà di scelta tra la richiesta di rilascio di una carta di identità cartacea o di una carta di identità digitale, entro dicembre 2018 il documento digitale sostituirà definitivamente quello cartaceo, come prescritto dal Piano triennale per l'Informatica nella Pubblica Amministrazione 2017-2019 e, ancor prima,

dalla **circolare del Ministero dell'Interno n. 18 del 19 ottobre 2016**, attraverso un piano di dispiegamento per l'abilitazione di tutti i comuni al rilascio della nuova CIE.
Tale nuova carta di identità porterà dei vantaggi rilevanti per i cittadini, in quanto è previsto che la stessa contenga anche il **codice fiscale** dell'intestatario, le **impronte digitali** e gli estremi dell'**atto di nascita**; ulteriore novità è costituita, poi, dalla possibilità di aggiungere alla memoria del microchip elettronico anche la volontà di essere **donatore di organi**, la propria tessera elettorale e l'abilitazione all'utilizzo dei servizi della Pubblica Amministrazione mediante l'inserimento della propria firma digitale.
L'art. 64 termina prescrivendo che, con futuro DPCM o DM, sarà stabilita la data a decorrere dalla quale i soggetti obbligati all'applicazione del C.A.D. (Pubbliche Amministrazioni, gestori di pubblici servizi e società a controllo pubblico) utilizzeranno **esclusivamente** le identità digitali ai fini dell'identificazione degli utenti dei propri servizi. Una disposizione, questa, che ricalca altre introdotte dal 2016 ad oggi e volte a dare un impulso finale al processo di digitalizzazione pubblico.

3.9 Istanze e dichiarazioni telematiche

La normativa vigente in tema di digitalizzazione prevede, all'**art. 65** del C.A.D., che le istanze e le dichiarazioni presentate telematicamente dal cittadino alle Amministrazioni e ai gestori di pubblici servizi siano da considerarsi valide:
a) se sottoscritte mediante **una delle forme di cui all'art. 20** (a parere di chi scrive, il richiamo del Legislatore a tutte le forme indicate nell'art. 20 può essere fuorviante e male interpretabile in funzione dell'intero contenuto dell'art. 65: in realtà, è lecito supporre che il Legislatore intendesse fare riferimento alle firme elettroniche avanzate, qualificate e digitali, oltre agli strumenti di identificazione informatica che, in base allo stesso art. 20, saranno meglio disciplinati con le future Linee Guida AgID; con esclusione quindi delle firme elettroniche semplici, utilizzabili per le istanze e dichiarazioni online del cittadino, ma con l'integrazione di quanto chiesto al punto c) dell'art. 65, di seguito esposto);
b) ovvero, quando l'istante o il dichiarante è identificato attraverso il **sistema pubblico di identità digitale (SPID)**, nonché attraverso **carta di identità elettronica (CIE)** o **carta nazionale dei servizi (CNS)**: in tali casi l'istanza è da intendersi come se fosse stata sottoscritta con **firma avanzata** in base all'art. 61, comma 2, del DPCM 22 febbraio 2013 (Regole tecniche firme avanzate ancor oggi efficaci) (la norma tecnica in questione non considera anche lo SPID, poiché non ricompreso, al tempo, nell'art. 65 C.A.D. cui la stessa fa riferimento ma, a seguito della

modifica dell'art. 65 avvenuta nel 2016, a parere di chi scrive, per analogia anche un'istanza o dichiarazione formulata con SPID deve oggi intendersi come se fosse stata sottoscritta con firma avanzata; conferma a tale impostazione deriva anche dal contenuto dell'art. 20 che affianca gli strumenti di identificazione informatica alle firme forti sotto il profilo della validità ed efficacia probatoria; è lecito supporre che, con le prossime Linee Guida AgiD in via di definizione, sarà chiarito espressamente questo punto);

c) ovvero sono **sottoscritte** e presentate **unitamente alla copia del documento d'identità**;

c-bis) ovvero se trasmesse dall'istante o dal dichiarante mediante la propria casella di **posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato (domicilio digitale)** purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee Guida AgID, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato: in tali casi l'istanza è da intendersi come se fosse stata sottoscritta con **firma avanzata** in base all'art. 61, comma 1, del DPCM 22 febbraio 2013 (Regole tecniche firme avanzate ancor oggi efficaci). In tal caso, **la trasmissione costituisce elezione di domicilio speciale ai sensi dell'art. 47 c.c.**: la dichiarazione del domicilio digitale vincola quindi il dichiarante e rappresenta espressa accettazione dell'invio da parte delle Pubbliche Amministrazioni, degli atti e dei provvedimenti che lo riguardano.

Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel **settore tributario**.

Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate validamente comporta **responsabilità dirigenziale e responsabilità disciplinare** dello stesso.

Le istanze e le dichiarazioni inviate con modalità telematiche sono da ritenersi **equivalenti** alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

Un'importante novità è stata prevista in tema di ricevuta dell'istanza.

A partire dall'1 gennaio 2017 le Pubbliche Amministrazioni devono adeguarsi al nuovo art. 18-bis della L. n. 241/1990 (introdotto dal D. Lgs. n. 126/2016) in materia di istanze, segnalazioni e comunicazioni presentate alle pubbliche amministrazioni anche in via telematica.

La norma prevede che:

- la **data di protocollazione** dell'istanza, segnalazione o comunicazione non può comunque essere diversa da quella di effettiva presentazione;
- dell'avvenuta presentazione di istanze, segnalazioni o comunicazioni deve essere rilasciata **immediatamente**, anche in via telematica, una **ricevuta**, che attesta l'avvenuta

presentazione dell'istanza, della segnalazione e della comunicazione e indica i termini entro i quali l'amministrazione è tenuta, ove previsto, a rispondere, ovvero entro i quali il silenzio dell'amministrazione equivale ad accoglimento dell'istanza.

Al fine di evitare eventuali illegittimità procedimentali, saggiamente il Legislatore prosegue nell'art. 18-bis specificando che le istanze, segnalazioni o comunicazioni **producono effetti anche in caso di mancato rilascio della ricevuta**, ferma restando la **responsabilità** del soggetto che avrebbe dovuto predisporla e non l'ha fatto. Se poi eventualmente l'istanza, segnalazione o comunicazione è stata inviata ad un **ufficio diverso** rispetto a quello effettivamente competente, i termini per la chiusura del procedimento decorrono comunque dalla ricezione da parte dell'ufficio competente.

Adeguarsi agli obblighi di cui all'art. 18-bis richiede di certo un'efficiente organizzazione dell'ufficio protocollo, e delle soluzioni informatiche di protocollo, ed un vero e proprio censimento delle istanze/segnalazioni/comunicazioni ricevute da ogni Pubblica Amministrazione ai fini della predisposizioni di format di ricevuta per ciascuna di esse e alla definizione delle modalità per il rilascio contestuale alla presentazione.

CAPITOLO 4
COMUNICAZIONI E TRASMISSIONI TELEMATICHE

4.1. Posta Elettronica Certificata

Per **posta elettronica certificata**, così come previsto dalle definizioni di cui all'art. 1 del CAD, si intende quel sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili a terzi. L'**efficacia probatoria** è equiparata a quella della raccomandata con avviso di ricevimento.

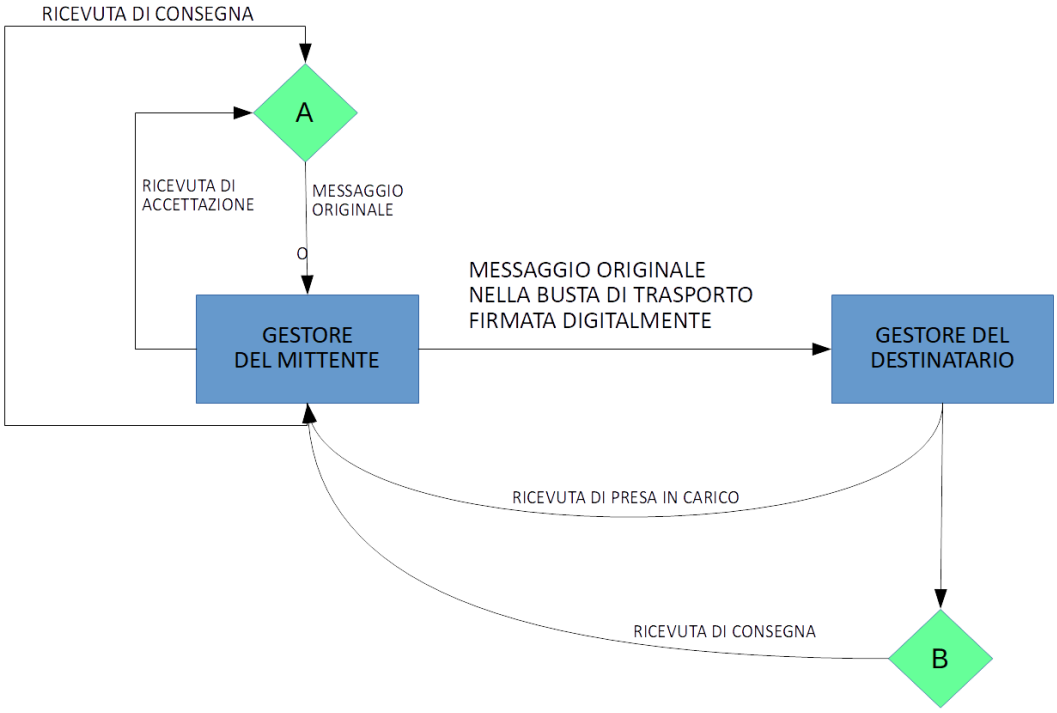
La normativa di riferimento per l'utilizzo e la validità delle trasmissioni di comunicazioni di posta elettronica certificata va ricercata, in particolare, nel D.P.R. n. 68 del 2005 e nel Decreto del Ministero per l'Innovazione e le Tecnologie contenenti le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata".

Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio con precisa indicazione temporale.

La certezza della provenienza e della integrità del messaggio di posta elettronica certificata è garantita dall'intermediazione del proprio gestore di posta elettronica che, verificata la correttezza

delle credenziali di accesso del mittente, imbusta il messaggio nella cosiddetta “busta di trasporto” e vi appone la propria firma digitale. Questa operazione consente di certificare ufficialmente l'invio e la consegna del messaggio.

Il gestore PEC del destinatario, alla ricezione, effettua un ulteriore controllo sulla validità della firma del gestore del mittente e provvede a prendere in carico il messaggio tentando la consegna al destinatario. A prescindere dall’esito positivo o negativo della consegna, il gestore del destinatario invia la ricevuta nella casella PEC del mittente.



In merito alle disposizioni che trattano della posta elettronica certificata all’interno del Codice dell’Amministrazione Digitale, in primo luogo si precisa che sensi dell’art. 1, comma n-ter), modificato seppur non sostanzialmente rispetto alla precedente stesura, un indirizzo elettronico eletto presso un servizio di posta elettronica certificata è idoneo a costituire un **domicilio digitale** valido per le comunicazioni elettroniche aventi valore legale.

Il riferimento al concetto di domicilio digitale ha, in qualche modo, superato nella nuova stesura del CAD il riferimento al solo indirizzo di posta elettronica certificata, tanto che con l’art. 7 comma 1 lett. a) del D.Lgs. 217/2017 è stata disposta la modifica anche della rubrica dell’art. 6 che da “Utilizzo della posta elettronica certificata” è stata modificata in “Utilizzo del domicilio digitale”. La posta elettronica certificata, pertanto, diviene solo uno dei mezzi idonei a costituire il domicilio digitale.

La ratio della modifica, come si legge anche nella nella Relazione illustrativa, è quella di inserire una definizione di domicilio digitale maggiormente in linea con la normativa europea e con i diritti di cittadinanza digitale.

Decreto Legislativo n. 82 del 7 marzo 2005 così come novellato dal D.Lgs. 217/2017	
Art. 6	
Testo previgente	Testo in vigore
Utilizzo della posta elettronica certificata	Utilizzo del domicilio digitale
1. Fino alla piena attuazione delle disposizioni di cui all'articolo 3-bis, per le comunicazioni di cui all'articolo 48, comma 1, 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.	1. Le comunicazioni tramite i domicili digitali sono effettuate agli indirizzi inseriti negli elenchi di cui agli articoli 6-bis, 6-ter e 6-quater, o a quello eletto come domicilio speciale per determinati atti o affari ai sensi dell'articolo 3-bis, comma 4-quinquies. Le comunicazioni elettroniche trasmesse ad uno dei domicili digitali di cui all'articolo 3-bis producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente. Le suddette comunicazioni si intendono spedite dal mittente se inviate al proprio gestore e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo. La data e l'ora di trasmissione e ricezione del documento

	informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.
1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni e' effettuata sulla base delle regole tecniche emanate da AgID, sentito il Garante per la protezione dei dati personali.	1-bis (abrogato)
	1-ter. L'elenco dei domicili digitali delle imprese e dei professionisti e' l'Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti di cui all'articolo 6-bis. L'elenco dei domicili digitali dei soggetti di cui all'articolo 2, comma 2, lettere a) e b), e' l'Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi, di cui all'articolo 6-ter. L'elenco dei domicili digitali delle persone fisiche e degli altri enti di diritto privato diversi da quelli di cui al primo e al secondo periodo e' l'Indice degli indirizzi delle persone fisiche e degli altri enti di diritto privato di cui all'articolo 6-quater.
	1-quater. I soggetti di cui all'articolo 2, comma 2, notificano direttamente presso i domicili digitali di cui all'articolo 3-bis i

	propri atti, compresi i verbali relativi alle sanzioni amministrative, gli atti impositivi di accertamento e di riscossione e le ingiunzioni di cui all'articolo 2 del regio decreto 14 aprile 1910, n. 639, fatte salve le specifiche disposizioni in ambito tributario. La conformità della copia informatica del documento notificato all'originale e' attestata dal responsabile del procedimento in conformità a quanto disposto agli articoli 22 e 23-bis.

Come già ampiamente argomentato nei precedenti capitoli, ai quale si rimanda per gli approfondimenti, la novità ha interessato anche gli art. 6-bis e 6-ter nei quali è stato riproposto il riferimento non più ai soli indirizzi PEC ma al domicilio digitale, nonché l'introduzione del nuovo art. 6-quater che tratta dell'indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese.

La decisione di sostituire il concetto di posta elettronica certificata con quello più ampio e completo di domicilio digitale è rinvenibile anche nell'art. 65 comma 7 del D.Lgs. 217/2017 che ha previsto l'abrogazione dell'art. 48 a decorrere dal 1 gennaio 2019. Il citato articolo 48, rubricato proprio "Posta elettronica certificata" prescrive che questo è il mezzo che deve essere utilizzato quando la trasmissione telematica di comunicazioni necessiti di una **ricevuta di invio** e di una **ricevuta di consegna**, o mediante altre soluzioni tecnologiche individuate con le Linee Guida. La trasmissione così effettuata equivale, salvo che la legge disponga diversamente, alla **notificazione a mezzo posta** e data ed ora di trasmissione e ricezione sono opponibili ai terzi se conformi alle disposizioni di cui al DPR n. 68/2005 e alle relative regole tecniche, ovvero conformi alle Linee guida.

È fatta salva comunque la possibilità di provare che la mancata consegna sia dovuta ad un fatto imputabile al destinatario della comunicazione.

La circostanza che l'art. 65 delle disposizioni transitorie preveda l'abrogazione dell'art. 48 non significa, ad ogni modo, che la PEC non sarà più riconosciuta come mezzo di comunicazione tra soggetti avente valore legale e opponibilità al terzo, posto che l'efficacia della PEC è comunque ricompresa nel concetto di "domicilio digitale" di cui al citato art. 6 comma 1 del CAD stesso.

L’art 1 del CAD, al comma 1-ter così come marginalmente modificato dall’ultimo correttivo, prescrive che se la legge consente l'utilizzo della posta elettronica certificata è da considerarsi ammesso anche l'utilizzo di altro **servizio elettronico di recapito certificato** purché sia **qualificato** ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.

Il regolamento eIDAS, ossia il Regolamento europeo n. 910 del 2014, all’art. 3 n. 36 definisce «servizio elettronico di recapito certificato» (SERC) un servizio che consenta la trasmissione di dati fra terzi per via elettronica e fornisca prove relative al trattamento dei dati trasmessi, tra cui prove dell’avvenuto invio e dell’avvenuta ricezione, e protegga i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.

Perché un siffatto servizio sia considerato come qualificato (SERCQ), deve soddisfare i requisiti prescritti dall’art. 44 del Regolamento eIDAS. In particolare:

- deve essere fornito da uno o più prestatori di servizi fiduciari qualificati;
- deve garantire con un elevato livello di sicurezza l’identificazione del mittente;
- deve **garantiscono l’identificazione del destinatario prima della trasmissione dei dati**;
- l’invio e la ricezione dei dati devono essere garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;
- qualsiasi modifica ai dati necessaria al fine dell’invio o della ricezione deve essere chiaramente indicata al mittente e al destinatario dei dati stessi;
- la data e l’ora di invio e di ricezione e qualsiasi modifica dei dati devono essere indicate da una validazione temporale elettronica qualificata.

È proprio la possibilità di identificazione del destinatario ciò che, oltre ai più elevati livelli di sicurezza, segna la differenza fondamentale tra la nostra PEC e lo standard SERCQ previsto a livello comunitario. Entrambi, ad ogni modo, sono idonei a costituire un valido domicilio digitale ai fini delle disposizioni del CAD.

L’apertura del legislatore nazionale verso lo standard comunitario potrebbe essere sintomo di un interesse, auspicato da molti, a migrare dal nostro sistema di posta elettronica certificata, singolare a livello europeo e caratterizzato da evidenti limitazioni di tipo tecnico (si pensi all’impossibilità di trasmettere allegati di dimensioni rilevanti), ad uno standard riconosciuto ed accettato oltre confine e caratterizzato da un livello di sicurezza più elevata oltre che da una migliore usabilità.

4.1.1. I gestori di posta elettronica certificata

I soggetti che intendono avviare l’attività di gestore di posta elettronica certificata, ai sensi del novellato art. 29 del CAD, devono presentare **domanda di qualificazione** all’AgID secondo le

modalità fissate dalle regole tecniche di indirizzo per l'attuazione del codice di cui all'art. 71. Viene meno, pertanto, l'obbligo di allegare una relazione tecnica sulla commercializzazione dei prodotti redatta da un organismo accreditato.

Per poter proporre domanda di qualificazione, il soggetto proponente deve avere natura giuridica di società di capitali, deve disporre dei requisiti di onorabilità, tecnologici e organizzativi e delle garanzie assicurative adeguate al volume di attività e alle responsabilità assunte nei confronti dei terzi. Inoltre, dovrà rispettare le condizioni previste dall'art. 24 del Regolamento eIDAS. I requisiti saranno individuati con decreto del Presidente del Consiglio dei ministri che, ai sensi del comma 8 dell'art. 65 del D.Lgs. 217/2017, dovrà essere emanato entro 180 giorni dall'entrata in vigore del predetto provvedimento. Sino ad a allora, resterà efficace il comma 3 dell'articolo 29 nella formulazione previgente all'entrata in vigore del correttivo.

In merito alle condizioni richieste dal comma 2 dell'art. 29, con provvedimento n.7221785 del 26 ottobre 2017, il **Garante per la Protezione dei dati personali**, nell'esprimere parere favorevole sullo schema del decreto legislativo recante le disposizioni integrative e correttive al d.lgs. 179/2016, aveva espresso, al punto 5, la necessità di porre l'accento sulle responsabilità che i soggetti richiedenti la qualificazione o l'accreditamento si assumono anche in riferimento al trattamento dei dati personali degli utenti. Il suggerimento del Garante, ad ogni modo, non ha trovato spazio nella stesura definitiva del correttivo che è rimasta invariata.

Decorsi 90 giorni dalla presentazione della domanda di qualificazione, qualora non sia stata comunicato al richiedente il provvedimento di diniego, la domanda si considera come accolta. Il termine può essere sospeso per una sola volte per richieste di integrazioni documentali che non siano già in possesso dell'AgID o che questa non possa acquisire in maniera autonoma. I soggetti che hanno ottenuto la qualificazione, verranno iscritti in un elenco pubblico tenuto dall'AgID e consultabile anche telematicamente.

La necessità, per i gestori di posta elettronica certificata, di dimostrare di avere idonee **garanzie assicurative** per l'attività svolta trova un corollario nell'art. 30 che ne sancisce la responsabilità in caso in cui cagionino danno ad altri nello svolgimento della propria attività con conseguente obbligo di provvedere al risarcimento di tutti i danni. Il gestore è liberato solo se riesce a dimostrare di aver adottato tutte le misure idonee ad evitare il danno.

Il mancato rispetto degli obblighi imposti ai gestori dalle disposizioni del codice o dal Regolamento eIDAS comporta, ai sensi dell'art. 32 bis, l'irrogazione da parte dell'AgID di una **sanzione amministrativa** che, a seconda della gravità della violazione, può variare da 40.000 a 400.000 euro, oltre al risarcimento dell'eventuale maggior danno. AgID provvederà, contestualmente

all'irrogazione della sanzione, a diffidare il gestore a conformarsi immediatamente alle disposizioni di legge.

Qualora la violazione sia considerata grave, come nel caso di condotte idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio, comportano la **cancellazione del fornitore dall'elenco dei soggetti qualificati** nonché il divieto di nuova qualificazione fino ai due anni successivi alla cancellazione..

È prevista anche la sanzione accessoria della pubblicazione della diffida o del provvedimento di cancellazione.

Analogo potere sanzionatorio è riconosciuto ad AgID nel caso in cui, a causa di un malfunzionamento non dovuto a causa di forza maggiore o caso fortuito, il servizio venga interrotto o il malfunzionamento non venga tempestivamente comunicato all'Agenzia e agli utenti. In questo caso, AgID potrà diffidare il prestatore del servizio invitandolo a ripristinare senza dilazione la regolarità della prestazione o a provvedere ad effettuare comunicazioni richieste. In caso di reiterazione nel biennio successivo alla prima violazione, si applica la sanzione della cancellazione dall'elenco pubblico.

Rispetto alla formulazione previgente dell'art. 32 bis, è evidente un inasprimento delle sanzioni. Basti pensare che fino all'entrata in vigore del correttivo, oltre a non essere previsto il divieto di qualificazione per un periodo successivo alla violazione e commisurato alla sua gravità, le sanzioni amministrative erano stabilite in un minimo di 4.000 ed un massimo di 40.000 euro. Appare evidente che il legislatore ha ritenuto di dover garantire in maniera più incisiva il rispetto delle disposizioni di settore, avuto riguardo anche all'importanza degli interessi in gioco e all'entità dei danni che potrebbero derivare da un comportamento illegittimo.

4.2. Trasmissione dei documenti tra Pubbliche Amministrazioni

Le modalità di trasmissione dei documenti tra le pubbliche amministrazioni sono disciplinate dall'art. 47 del CAD.

Tale disposizione non ha subito importanti modifiche con l'entrata in vigore del nuovo correttivo, se non limitatamente al terzo comma, in quanto sono stati apportati minimi aggiustamenti per proseguire l'opera di razionalizzazione e coordinamento delle disposizioni.

La norma in oggetto dispone che le comunicazioni tra le Pubbliche Amministrazioni debbano avvenire mediante modalità telematica ed, in particolare, mediante "l'utilizzo della **posta elettronica** o in **cooperazione applicativa**". Una terza via è quella di rendere disponibile un atto o un documento comunicando al destinatario le **modalità di accesso telematico** allo stesso. In questo

contesto, le comunicazioni dei documenti sono valide ai fini del procedimento amministrativo solo qualora sia possibile verificarne la provenienza e a partire dal momento della verifica.

Va sottolineato, a tale scopo, che in caso di comunicazione mediante posta elettronica, non è richiesto necessariamente che sia utilizzato un indirizzo certificato, ma è sufficiente l'uso della posta elettronica ordinaria. È, però, previsto un ulteriore elemento affinché possa essere accertata la validità della comunicazione ai fini del procedimento amministrativo, ossia la **verifica della provenienza** dei documenti.

Perché la provenienza dei documenti possa considerarsi verificata, ai sensi dell'art. 47 comma 2, è necessario che le comunicazioni soddisfino uno dei seguenti requisiti:

- siano sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- siano dotate di segnatura di protocollo che consiste nell'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, della informazioni riguardanti il documento stesso e ne consente l'individuazione in modo inequivocabile;
- siano trasmesse mediante sistemi di posta elettronica certificate.

È altresì fatta salva (lett. c) la possibilità di accertare in altro modo la provenienza facendo riferimento alla normativa vigente o alle Linee Guida, fermo restando il **divieto di trasmissione di documenti a mezzo fax**.

Lascia ancora qualche perplessità la collocazione di quest'ultima disposizione nel comma relativo alla verifica della provenienza delle trasmissioni documentali tra pubbliche amministrazioni, in quanto poco chiara e già in passato veicolo di equivoci interpretativi in merito alla sua effettiva portata sulla possibilità o meno, per le pubbliche amministrazioni, di mantenere l'utilizzo del fax per usi estranei alla comunicazione tra pubbliche amministrazioni o per comunicazioni per le quali non sia necessariamente richiesta la verifica della provenienza.

Ad ogni modo, il mancato rispetto di tali prescrizioni comporta una **responsabilità dirigenziale** e **disciplinare** oltre che per **danno erariale** nel caso in cui sia configurabile.

Al fine di rendere più agevole le comunicazioni tra amministrazioni, le pubbliche amministrazioni e i gestori di servizi pubblici, di cui all'art. 2 comma 2, lett. a) e b), sono tenuti ad istituire e pubblicare nell'**indice dei domicili digitali** almeno una casella di posta elettronica certificata per ogni registro di protocollo. Restano escluse da questo obbligo, per espressa previsione normativa, le società a controllo pubblico di cui alla lett. c) del citato articolo.

Ovviamente l'art. 47 deve essere letto in combinato disposto con l'art. 48 del Codice che prescrive, se non altro fino al 1 gennaio 2019, che sia mantenuto l'uso della posta elettronica certificata tutte le volte in cui sia necessario avere una ricevuta di invio e una ricevuta di consegna.

Nell'ambito del Capo IV sulla "Trasmissione informatica dei documenti" vengono in rilievo altre due disposizioni che sono applicabili alle comunicazioni tra pubbliche amministrazioni.

La prima l'art. 46 la quale prevede che, al fine di garantire la riservatezza dei dati sensibili o giudiziari, i documenti informatici trasmessi ad altre pubbliche amministrazione per via digitale possono contenere soltanto i **dati sensibili e giudiziari consentiti dalla legge** o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

I dati personali, come risulta dalla definizione del D.Lgs. 196/2003, sono quelli idonei a 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale dell'interessato; sono invece dati giudiziari quei dati personali dai quali si possa evincere l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o indagato.

L'art. 49 del codice, invece, estende, qualora ve ne fosse bisogno, il **principio della segretezza** anche alla corrispondenza trasmessa per via telematica. È fatto divieto, in funzione della predetta norma, agli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici, di prendere cognizione della corrispondenza telematica, di duplicarla con qualsiasi mezzo o di 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.

Il secondo comma, a chiusura della disposizione, sancisce che gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

4.3. Protocollo informatico e gestione documentale digitale

L'introduzione del concetto di protocollo informatico nella pubblica amministrazione italiana risale al 2000 quando, con il Decreto del Presidente della Repubblica n. 445/2000, ne statuì l'obbligo di adozione entro il termine del 1 gennaio 2004, conformemente alle linee guida all'epoca in vigore.

L'evoluzione che ne è seguita ha portato ad un mutamento sostanziale: si è passati dalla mera **digitalizzazione** del protocollo cartaceo alla necessità di implementare un sistema di protocollo informatico perfettamente integrato e sincronizzato con quello di **gestione documentale** e di **conservazione**.

Pertanto, la **dematerializzazione** documentale prevista dall'attuale quadro normativo non può prescindere dall'implementazione, da parte delle amministrazioni, di adeguati sistemi per la gestione documentale ed il protocollo informatico. È quanto prevede l'art. 50 del citato D.P.R., che impone alle pubbliche amministrazioni di realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi, individuando, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.

Come previsto dallo stesso articolo, inoltre, le amministrazioni hanno l'obbligo di progettare e gestire i propri sistemi in ottemperanza alla normativa in materia di riservatezza dei dati personali.

La **gestione dei flussi documentali** è l'insieme di funzionalità che consentono di gestire e organizzare la documentazione ricevuta e prodotta dalle amministrazioni, garantendo la corretta registrazione di protocollo, l'assegnazione, la classificazione, la fascicolazione, il reperimento e la conservazione dei documenti informatici. Il sistema di gestione informatica dei documenti, a norma dell'art. 52 del D.P.R. n. 445/2000, deve essere strutturato in modo tale da garantire la sicurezza e l'integrità del sistema stesso; garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita; fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali; consentire il reperimento delle informazioni riguardanti i documenti registrati; consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali; garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Inoltre, per una corretta gestione documentale, è lo stesso Codice dell'Amministrazione Digitale a prevedere che le pubbliche amministrazioni siano tenute - per ciascun procedimento amministrativo di loro competenza - a raccogliere in un **fascicolo informatico** gli atti e i documenti da chiunque formati, rendendoli direttamente consultabili ed alimentabili da tutte le amministrazioni coinvolte nel procedimento.

Il D.Lgs. 217/2017 ha poi introdotto la **pari accessibilità al fascicolo informatico da parte di tutti gli interessati** attraverso il sistema documentale di ricerca, di cui si dirà appresso, ed il punto di accesso telematico ai servizi della pubblica amministrazione.

A norma dell'art. 41, comma 2-ter del CAD, così come modificato dall'ultimo correttivo, il fascicolo informatico deve recare l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;
d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
f) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida.

Come accennato, il **D.Lgs. n. 217/2017** ha introdotto l'**art. 40-ter** del CAD che ha previsto il **Sistema pubblico di ricerca documentale**. Si tratta di un sistema "volto a facilitare la ricerca dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e di cui all'articolo 40-bis e dei fascicoli dei procedimenti di cui all'articolo 41, nonché a consentirne l'accesso on-line ai soggetti che ne abbiano diritto ai sensi della disciplina vigente". Le amministrazioni sono tenute, dunque, ad integrare il proprio servizio di gestione documentale con il sistema di ricerca documentale, al fine di consentire - attraverso una corretta indicizzazione dei files - la ricerca dei documenti soggetti ad obblighi di pubblicità legale nonché la consultazione e l'alimentazione dei fascicoli informatici da parte delle amministrazioni coinvolte nei procedimenti e dei soggetti interessati.

4.3.1. Il nucleo minimo del protocollo informatico

Per nucleo minimo del protocollo si intende la **componente applicativa** che realizza le funzioni di registrazione di protocollo, segnatura e classificazione dei documenti ricevuti ed inviati. Tali operazioni rappresentano il presupposto richiesto per l'attuazione di sistemi di gestione documentale a norma.

Il protocollo è costituito da un registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'**identificazione univoca** del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.

L'operazione di registrazione di protocollo deve essere effettuata per ogni documento ricevuto o spedito dalle pubbliche amministrazioni mediante la memorizzazione delle informazioni previste dall'**art. 53** del D.P.R. n. 445/2000, ossia:

a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;

b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;

c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;

d) oggetto del documento, registrato in forma non modificabile;

e) data e protocollo del documento ricevuto, se disponibili;

f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Inoltre, l'art. 40-bis del CAD, così come modificato dal D.Lgs. n. 217/2017 al fine di razionalizzare la disposizione con l'introduzione del concetto di domicilio digitale, dispone che: «Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida».

Il protocollo informatico, in tale contesto, riveste un ruolo strategico, realizzando le condizioni operative per un'efficace ed efficiente gestione del flusso informativo e documentale interno delle pubbliche amministrazioni. Un sistema di protocollo e gestione documentale ben strutturato permette, inoltre, di attuare concretamente i principi dettati dalla **L. n. 241/1990** in materia di **trasparenza** dell'azione amministrativa e snellimento delle procedure.

In tema di registrazione di protocollo va sottolineato l'obbligo delle pubbliche amministrazioni di inserire una serie di informazioni all'interno del **manuale di gestione**. Tale documento, come previsto dal **D.P.C.M. 3 dicembre 2013**, deve riportare:

- l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce;
- l'indicazione delle unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea; l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 53, comma 5, del testo unico;
- l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento;
- le modalità di produzione e di conservazione delle registrazioni di protocollo informatico e, in particolare, l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione

di segnatura ai sensi dell’art. 55 del Testo unico, nonché le modalità di registrazione delle informazioni annullate o modificate nell’ambito di ogni sessione di attività di registrazione.

L’art. 18 del DPCM 3 dicembre 2013 prescrive ulteriori obblighi per le pubbliche amministrazioni. Ed infatti, ad ogni messaggio ricevuto o spedito da una area organizzativa omogenea deve corrispondere un’unica operazione di registrazione di protocollo. Alla registrazione di protocollo devono essere associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione.

Ciascuna amministrazione, poi, è tenuta ad istituire, per ogni area organizzativa omogenea, almeno una casella di posta elettronica certificata direttamente associata al registro di protocollo, ai sensi del già citato art. 46 comma 3 del Codice, da utilizzare per la protocollazione dei messaggi ricevuti e spediti. L’indirizzo di tali caselle è riportato nell’indice dei domicili digitali delle amministrazioni e nel manuale di gestione di cui all’art. 5, nonché pubblicato sul sito dell’amministrazione. È fatta salva, ovviamente, la facoltà per ciascuna amministrazione di istituire specifiche caselle di posta elettronica, anche certificata, per trattare peculiari tipologie documentali, anche oggetto di registrazione particolare. Gli indirizzi di tali caselle sono anch’essi soggetti agli obblighi di pubblicazione dell’indice dei domicili digitali, nel manuale di gestione e sul sito dell’amministrazione.

Qualora i documenti informativi pervengano ad un’area organizzativa omogenea, è l’amministrazione stessa a dover decidere, secondo quanto previsto dallo stesso manuale di gestione, quali documenti sono oggetto di registrazione di protocollo o di registrazione particolare. Il manuale di gestione, inoltre, deve prevedere anche le scelte dell’amministrazione in merito alla modalità di inoltro e assegnazione dei documenti al singolo ufficio.

Inoltre, se nel documento è indicato un ufficio utente o il soggetto destinatario, questo va riportato nella segnatura di protocollo. Per **segnatura di protocollo** si intende l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime che la segnatura deve associare sono i codici identificativi dell’amministrazione, dell’area organizzativa omogenea e del registro nonché la data e il progressivo di protocollo.

Le operazioni di segnatura e registrazione di protocollo devono essere svolte in contemporanea. Nel caso in cui siano già disponibili al momento della registrazione di protocollo, l’operazione di segnatura di protocollo può includere il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del

documento e ogni altra informazione utile o necessaria. Il D.P.C.M. 3 dicembre 2013 disciplina le specifiche tecniche che i dati relativi alla segnatura di protocollo devono rispettare.

Nel caso in cui occorra annullare una o più informazioni assegnate o generate automaticamente dal sistema e registrate in forma immodificabile, è necessario che i sistemi delle amministrazioni determinino l'automatico e contestuale annullamento dell'intera registrazione di protocollo (art. 8, D.P.C.M. 3 dicembre 2013). Quando, invece, sia necessario correggere errori intercorsi in sede di immissione di dati delle altre informazioni, i sistemi devono permettere tale operazione, memorizzando, però, in modo permanente, il valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica.

4.3.2. Requisiti di sicurezza

La determinazione dei requisiti di sicurezza che i sistemi di protocollo informatico delle amministrazioni devono garantire, è affidata all'art. 7. del DPCM 3 dicembre 2013. In particolare, i sistemi di protocollo informatico devono assicurare:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Lo stesso articolo prevede, inoltre, che il sistema di protocollo informatico consenta il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti e il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Una importante misura di sicurezza è rappresentata dall'**obbligo di trasmettere il registro giornaliero di protocollo** entro la giornata lavorativa successiva al sistema di conservazione, al fine di garantire l'immodificabilità del contenuto.

Infine, il sistema di protocollo deve rispettare le misure di sicurezza previste dal Codice in materia di protezione dei dati personali agli articoli 31 e 36 nonché nel disciplinare tecnico di cui all'allegato B.

Nello specifico, l'art. 31 del cosiddetto Codice privacy, recante la rubrica Obblighi di sicurezza, prescrive che i dati personali oggetto di trattamento siano custoditi e controllati 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. Le misure di sicurezza devono essere commisurate alle

conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento.

L'art. 36, invece, richiamando il citato disciplinare tecnico relativo alle misure minime, ne prescrive il periodico aggiornamento 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.

Ad oggi il **Disciplinare tecnico in materia di misure minime di sicurezza** dispone che il titolare, il responsabile, ove designato, e l'incaricato debbano adottare, in caso di trattamento dei dati con strumenti elettronici, alcune modalità tecniche. In primo luogo, un sistema di **autenticazione informatica**, ossia un codice per l'identificazione dell'incaricato associato ad una password (credenziali di autenticazione) oppure un **dispositivo di identificazione** o, infine, un **dato biometrico** dell'incaricato, associati o meno a delle credenziali di autenticazione. Il disciplinare prevede anche la possibilità di utilizzare un **sistema di autorizzazione** così da consentire a ciascun incaricato l'accesso ai soli dati necessari per effettuare le operazioni di trattamento cui è preposto.

Nei prossimi mesi si renderà, ad ogni modo, necessario un importante lavoro di razionalizzazione della normativa vigente in materia di misure di sicurezza nel trattamento dei dati personali avuto riguardo all'imminente piena applicazione del Regolamento europeo (UE) 2016/679, prevista per il 25 maggio 2018, e all'emanazione del necessario decreto legislativo di adeguamento della normativa nazionale alle disposizioni comunitarie.

4.3.3. Il manuale di gestione

Il Manuale di gestione del protocollo informatico è il documento previsto dal DPCM 3 dicembre 2013 (Regole tecniche per il protocollo informatico) che ha l'obiettivo di descrivere il **sistema di gestione**, anche ai fini della conservazione, dei documenti informatici e fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Spetta al Responsabile della gestione documentale (ovvero al coordinatore della gestione documentale, ove previsto) predisporre lo schema del manuale che poi sarà soggetto all'approvazione dall'amministrazione e alla pubblicazione sul sito istituzionale.

Il contenuto del manuale di gestione è statuito dall'art. 5 delle regole tecniche, che prevede che nel documento siano riportati:

a) la pianificazione, le modalità e le misure di cui all'art. 3, comma 1, lettera e) ;
b) il piano di sicurezza dei documenti informatici di cui all'art. 4, comma 1, lettera c);

c) le modalità di utilizzo di strumenti informatici per la formazione dei documenti informatici, ai sensi dell'art. 40, comma 1, del Codice, e per lo scambio degli stessi all'interno ed all'esterno dell'area organizzativa omogenea, ivi comprese le caselle di posta elettronica, anche certificata, utilizzate;
d) la descrizione di eventuali ulteriori formati utilizzati per la formazione del documento informatico in relazione a specifici contesti operativi esplicitati e motivati;
e) l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce;
f) la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione, tra i quali, in particolare, documenti informatici pervenuti attraverso canali diversi da quelli previsti dagli articoli 16 e 17, nonché tramite fax, raccomandata o assicurata;
g) l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
h) le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;
i) l'indicazione delle unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea;
j) l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'art. 53, comma 5, del testo unico;
k) l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento;
l) i registri particolari definiti per il trattamento di registrazioni informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, di cui all'art. 40, comma 4, del Codice;
m) il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;
n) le modalità di produzione e di conservazione delle registrazioni di protocollo informatico e, in particolare, l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione

di segnatura ai sensi dell'art. 55 del Testo unico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione;

o) la descrizione funzionale ed operativa del componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti con particolare riferimento alle modalità di utilizzo;
p) i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;
q) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del testo unico, inclusa la funzione di recupero dei dati protocollati manualmente.

4.4. Semplificazione e digitalizzazione dei processi amministrativi

L'art. 3 bis della legge 241/1990, così come introdotto dell'art. 3 legge 15 del 2015, ha sancito già molti anni fa un assunto particolarmente importante per il processo di cambiamento già allora in atto, ossia che l'efficienza della pubblica amministrazione passava necessariamente per l'introduzione degli strumenti digitali nei rapporti tra amministrazioni e tra queste e i privati.

Con il passare degli anni e con il delinearsi delle esigenze di interoperabilità, cooperazione e connettività è emerso come la digitalizzazione della pubblica amministrazione non potesse essere limitata esclusivamente alle infrastrutture tecnologiche e all'uso dei relativi strumenti, ma dovesse passare necessariamente per una revisione dell'intero processo amministrativo strutturato in un'ottica di semplificazione resa possibile dai nuovi strumenti a disposizione.

L'art. 12 comma 1 del CAD prevede, infatti, che le pubbliche amministrazioni, nel perseguimento dei propri obiettivi, organizzino l'attività di competenza in autonomia; la disposizione va però letta in combinato disposto con l'art. 15 che, al comma 1, a sua volta fa riferimento ad una **strategia coordinata** di riorganizzazione strutturale e gestionale delle pubbliche amministrazioni che garantisca il coerente sviluppo del processo di digitalizzazione.

In questa ottica, le pubbliche amministrazioni, come previsto dal comma 2 del medesimo articolo, provvedono a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle Linee guida.

Appare chiaro, pertanto, che la semplificazione della PA debba necessariamente passare attraverso un lavoro di modifica dei procedimenti che sia il più omogeneo possibile, così da perseguire gli obiettivi di cui all'art. 12 anche attraverso cooperazione e interoperabilità. Appare ancor più chiaro, pertanto, che si renda necessaria una **compressione di quella autonomia operativa** alla base

dell’azione amministrativa, in favore di una necessaria ed imprescindibile standardizzazione dei processi.

Negli ultimi anni il processo di digitalizzazione e semplificazione della pubblica amministrazione ha cercato di perseguire, non sempre riuscendo nell’intento, il raggiungimento di importanti obiettivi in settori considerati nevralgici. Uno fra tutti, la piena attuazione della **cittadinanza digitale** con la messa a disposizione di un sempre maggior numero di servizi online oltre che attraverso la fruibilità di documenti di interesse in modalità telematica. Le modalità di attuazione sono passate attraverso la diffusione del Sistema Pubblico di Identità Digitale (SPID), l’implementazione dei pagamenti elettronici, il tentativo di piena digitalizzazione del processo civile, amministrativo e tributario.

Sicuramente né i risultati né le tempistiche sono stati quelli sperati anche perché i propositi riformatori del legislatore si sono dovuti necessariamente scontrare con ostacoli non sempre facili da superare e che riguardano direttamente la digitalizzazione della pubblica amministrazione, ossia il cosiddetto digital divide e la necessità di salvaguardare in maniera estremamente efficace la sicurezza dei dati.

4.5. Continuità operativa, interoperabilità e cooperazione applicativa

4.5.1. La continuità operativa nel nuovo art. 51 e la sicurezza dei dati

Nel corso degli anni e dell’evoluzione del CAD, si è assistito a evidenti cambi di rotta del legislatore in merito a concetti chiavi nella digitalizzazione del Paese, seguiti da vuoti nelle previsioni normative e dalla necessità di armonizzare le disposizioni riforma dopo riforma.

Sicuramente questo è ciò che è successo in merito alle previsioni sulla **continuità operativa** ossia, in sintesi, sulla procedura che ogni pubblica amministrazione dovrebbe porre in essere per ripristinare, in caso di interruzione imprevista, il servizio prestato, per salvaguardare l’integrità dei dati e degli applicativi e per ritornare, da ultimo, alla normale funzionalità.

Il primo intervento normativo di rilievo è stato effettuato dal legislatore con D.Lgs. 235/2010, con il quale era stata disposta l’introduzione dell’art. 50-bis, rubricato, appunto “Continuità operativa”. La disposizione prevedeva che, preso atto dei profili di rischio dovuti alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, ciascuna pubblica amministrazione dovesse predisporre, in autonomia e con il controllo del Ministero preposto e dell’AgID, adeguati **piani di emergenza** in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

Nel dettaglio, alle pubbliche amministrazione era demandata la definizione del cosiddetto piano di continuità operativa, con obiettivi, misure preventive e procedure standardizzate da seguire tenendo

conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche, nonché il piano di disaster recovery sulle misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

La previsione normativa aveva da subito suscitato molte perplessità proprio sulla effettiva attuabilità di un siffatto proposito, avuto riguardo alla complessità del compito rispetto alle concrete risorse, anche in termini di competenza, delle singole amministrazioni.

Le difficoltà applicative devono aver convinto anche il legislatore, tanto che l'art. 50-bis è stato abrogato con l'entrata in vigore del D.Lgs. 179/2016 e le sue previsioni hanno trovato nuova formulazione nei commi dell'**art. 51** così come modificato a seguito dell'ultimo correttivo.

L'art. 51 sulla sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni prescrive che le soluzioni tecniche più idonee a garantire, tra l'altro, la continuità operativa siano individuate con le Linee guida. Il compito di individuare le migliori soluzioni per far fronte agli incidenti di sicurezza informativi e di predisporre i programmi di sicurezza preventiva è affidato ad AgID, di concerto con le altre autorità competenti in materia, mentre le amministrazioni pubbliche, i gestori di servizi pubblici e le società a controllo pubblico sono tenuti ad aderirvi ogni anno e a predisporre piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività.

Un elemento di concreta novità può essere rinvenuto nel comma 2 quater il quale prevede che le amministrazioni, al fine di concretizzare gli impegni prescritti nei commi precedenti, possano stringere **accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune** quali, in questo caso, l'erogazione di servizi applicativi, infrastrutturali e di dati, con ristoro dei soli costi di funzionamento, ai sensi dell'art. 15 della legge 241/1990. Intento di quest'ultima previsione, seppur non esplicitato nell'articolo ma chiaramente emergente dalla relazione illustrativa, sarebbe quello di permettere la fruizione di servizi a tecnologia evoluta disponibili presso i poli di eccellenza pubblici da parte degli enti che non dispongano di risorse umane ed economiche sufficienti a garantire lo standard minimo di sicurezza fissato dalle Linee guida AgID e richiesto dagli organismi internazionali. Questo permetterebbe anche alle amministrazioni più deboli sul fronte della sicurezza, di usufruire di soluzioni altrimenti inaccessibili e contribuire, così, all'innalzamento del livello complessivo di sicurezza della pubblica amministrazione.

La necessità che vengano implementati i sistemi di sicurezza e garantite procedure efficaci di ripristino dei sistemi è, senza ombra di dubbio, strettamente connessa non solo all'interesse alla continuità dei servizi prestati, bensì anche e soprattutto alla **protezione della incredibile mole di dati** che vengono raccolti e che transitano nelle infrastrutture informatiche della pubblica amministrazione. L'art. 51, ad ogni modo, prevede un semplice accenno alla necessità che i

documenti informatici delle pubbliche amministrazioni debbano essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta (comma 2).

È lasciato alle Linee guida e, ovviamente, alla normativa di settore, l'individuazione delle soluzioni tecniche più idonee a garantire la protezione, l'integrità e la riservatezza dei dati. Si evidenzia, ad ogni modo, che il Garante per la protezione dei dati personali, con parere n. 7221785 del 27 ottobre 2017, ha sollevato alcune perplessità sull'opportunità di demandare alle Linee guida di cui all'art. 71 il compito di fornire prescrizioni di natura cogente in tema di sicurezza e protezione dei dati personali. A parere del Garante, lo strumento delle "regole tecniche" è da considerarsi come maggiormente adeguato alla regolazione di un ambito come quello della sicurezza dei dati e della loro concreta protezione, anche e soprattutto innanzi alla rapidissima evoluzione tecnologica e ai rischi ad essa connessa.

4.5.2. Cooperazione applicativa e interoperabilità nella comunicazione e trasmissione di documenti

Alla base dell'amministrazione digitale e del principio di cooperazione tra le vari pubbliche amministrazioni ci sono i concetti di **interconnessione** e **interoperabilità**. L'art. 12 del Codice, in merito alle norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa, al comma 2 prevede la garanzia di interoperabilità dei sistemi e l'integrazione dei processi di servizio nei rapporti interni, con altre amministrazioni o con i privati.

Abbiamo già accennato alla **cooperazione applicativa** come ad una delle possibili modalità di comunicazione tra Pubbliche Amministrazioni di cui all'art. 47 del Codice. La definizione è contenuta nel dettato dell'art. 72, comma 1 lett. e) che descrive la descrive come quella "parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informativi dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e dei procedimenti amministrativi". Lo scopo della cooperazione applicativa è, pertanto, quello di permettere l'integrazione dei processi e dei dati di amministrazioni diverse. Ciò al fine di gestire i procedimenti amministrativi in modo unitario e persino contestuale, con risparmio di tempo e risorse.

Il sistema di cooperazione applicativa attiene, pertanto, all'aspetto prettamente tecnico e delle infrastrutture delle pubbliche amministrazioni. Può essere descritto come un insieme di sistemi informatici appartenenti allo stesso soggetto o anche a soggetti diversi che hanno la possibilità di interagire tra di loro in maniera diretta, non mediata da interventi esterni e automatica.

Da quanto sin qui esposto appare evidente perché la regolamentazione del sistema sia necessariamente demandata all'emanazione di linee guida, regole tecniche e di sicurezza volte a delinearne le caratteristiche ed il funzionamento.

All'interno del CAD i riferimenti diretti al concetto di cooperazione applicativa, seppure generali e di larga applicazione, sono pochi in quanto, appunto, la sua realizzazione della deve essere il fine delle scelte procedimentali e non effettuate dalla pubblica amministrazione. Ne tratta, oltre all'art. 47 già citato, anche l'art. 68 sull'analisi comparativa delle soluzioni che, appunto, devono tendere a garantire l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione.

Il concetto di cooperazione applicativa riguarda, in particolar modo, la disponibilità dei dati della pubblica amministrazione. L'art. 43 del D.Lgs. 217/2017 ha inserito nell'art. 50 del Codice il comma 2-bis secondo cui le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, devono procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti di cui all'articolo 2, comma 2. Si precisa, poi, che la predetta attività dovrà essere svolta secondo le modalità individuate dall'AgID con le Linee guida. Dalla relazione illustrativa si evince che le citate linee guida "chiariranno negli aspetti tecnologici il funzionamento dei modelli di cooperazione applicativa, tenendo conto del necessario aggiornamento tecnico per consentire di beneficiare, in una logica di sistema, del progresso tecnologico creando adeguate condizioni di economicità ed efficienza. Tali nuove previsioni rispondono alla duplice esigenza da una parte di valorizzare il patrimonio informativo delle amministrazioni e dall'altra di superare le attuali 17 modalità operative attraverso le quali le amministrazioni condividono i dati personali dei quali sono titolari con un nuovo approccio basato sul dialogo c.d. machine to machine tra i sistemi delle diverse amministrazioni".

Il risultato di un sistema connesso in cooperazione applicativa, come avviene, ad esempio, per i più recenti sistemi di pagamento verso le pubbliche amministrazioni (si veda l'art. 5 del Codice), è quello di un unico sistema integrato ed interoperabile, costituito da parti che fanno capo a soggetti diversi ma, allo stesso modo, che cooperano tra loro.

Perché la cooperazione sia efficiente ed efficace è, ad ogni modo, necessario il rispetto delle regole per l'interoperabilità. L'art. 1 del nuovo CAD definisce **interoperabilità** quella caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, capace di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi. Lo scambio di informazioni e, pertanto, l'accessibilità continuativa e contestuale a tutti i documenti a disposizione delle diverse pubbliche amministrazioni, garantisce senza ombra di dubbio anche sotto il profilo tecnico una garanzia di completezza dell'istruttoria, celerità del procedimento

amministrativo e possibilità di reale partecipazione da parte dei soggetti pubblici e privati. Ciò garantisce, inoltre, che non vi siano lacune informative o difformità nella comunicazione dei dati e, per l'effetto, dà la certezza di avere un sistema efficiente.

Il modello di interoperabilità fino ad oggi applicato era basato sulle regole tecniche emanate sino al 2008. Con il Piano triennale per l'informatica nella Pubblica amministrazione 2017-2019, approvato dal Presidente del Consiglio dei Ministri il 31 maggio 2017, è stato previsto il passaggio ad un nuovo modello, maggiormente efficace e sostenibile, di interoperabilità che sarebbe dovuto essere definito con linee guida entro la fine del 2017. Ad oggi, le nuove linee guida non sono state ancora emanate e, pertanto, nell'attesa resta applicabile il documento, anch'esso previsto dal Piano triennale, recante "Linee guida per transitare al nuovo Modello di interoperabilità" e pubblicato il 2 agosto 2017.

4.6. Sistema Pubblico di Connettività

Nell'ottica del Codice dell'Amministrazione Digitale, la pubblica amministrazione dovrebbe operare come un sistema in cui le amministrazioni centrali e territoriali, collegate in un'unica rete, agiscono in sintonia grazie allo scambio di informazioni, documenti e dati per via telematica.

A questo sistema, chiamato Sistema Pubblico di Connettività e Cooperazione (SPC), è dedicato l'intero Capo VIII che, successivamente all'entrata in vigore del D.Lgs. 179/2016, ha visto abrogati la maggior parte degli articoli che lo componevano in un intento di semplificazione e razionalizzazione della disciplina. Ad oggi, infatti, sono ancora in vigore esclusivamente gli artt. 73, 75, 76 e 76 bis.

L'art. 73 ci fornisce la definizione di Sistema Pubblico di Connettività e Cooperazione ossia l'insieme di infrastrutture, architetture e interfacce tecnologiche, linee guida e regole tecniche, servizi e applicazioni, che assicura l'**interoperabilità** tra i sistemi informativi delle pubbliche amministrazioni e la cooperazione a livello applicativo; permette il **coordinamento informativo e informatico** dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea ed è aperto all'adesione da parte dei gestori di servizi pubblici e dei soggetti privati.

Al Sistema Pubblico di Connettività e Cooperazione è demandata la garanzia della sicurezza e della riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascun soggetto aderente.

La realizzazione del Sistema avviene tenendo conto dei seguenti principi: lo sviluppo architetturale e organizzativo atto a garantire la federabilità dei sistemi, economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa, aggiornamento continuo del

sistema e aderenza alle migliori pratiche internazionali, sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione (art. 73, comma 3). È, invece, rimesso all'emanazione di regole tecniche, ai sensi dell'art. 71, il dettaglio sul funzionamento del Sistema al fine di assicurarne nel tempo l'adeguamento all'evoluzione della tecnologia, alle disposizioni comunitarie e alle esigenze pratiche delle pubbliche amministrazioni.

Le pubbliche amministrazioni, i gestori di servizi pubblici e le società a controllo pubblico partecipano al Sistema pubblico di connettività, fatte salve le esclusioni collegate all'esercizio delle funzioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali.

Nel rispetto delle regole tecniche, chiunque può partecipare al SPC e ciò è reso possibile dalla condivisione gratuita, da parte di AgID, delle specifiche delle interfacce tecnologiche, delle linee guida, delle regole di cooperazione e di ogni altra informazione necessaria a garantire l'interoperabilità del SPC con ogni soluzione informatica sviluppata autonomamente da privati o da altre amministrazioni che rispettano le regole definite ai sensi dell'articolo 73, comma 3-quater.

I costi riferibili alle infrastrutture del SPC, ai sensi dell'art. 76-bis, sono suddivisi tra i fornitori per i servizi da essi direttamente utilizzati e in proporzione agli importi dei contratti di fornitura, e le pubbliche amministrazioni che sostengono i costi dei servizi effettivamente utilizzati.

CAPITOLO 5
CONSERVAZIONE DIGITALE

5.1. La conservazione digitale: profili generali.

Con l'espressione conservazione digitale si definisce quell'insieme di attività finalizzate a conservare i documenti in formato digitale, consentendo di garantirne l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità (art. 44, comma 1-ter, CAD). Si tratta, in altri termini, di una procedura informatica che permette, nel rispetto dei requisiti previsti dalla normativa di settore, di gestire i documenti informatici, garantendone nel tempo la validità legale.

La conservazione digitale dei documenti rappresenta, d'altra parte, un processo essenziale nel più generale fenomeno della dematerializzazione, assicurando che i documenti e le informazioni rimangano a disposizione per un periodo di tempo astrattamente indeterminato, attraverso formati digitali che diano garanzie di autenticità e accessibilità dei contenuti.

Peraltro, la conservazione dei documenti è una funzione di carattere istituzionale per tutte le pubbliche amministrazioni, tenute a conservare e preservare i propri atti e documenti da ogni alterazione e/o sottrazione, siccome concernenti diritti e interessi pubblici e privati.

I soggetti privati, quali le società o i singoli individui che svolgono un'attività economica, sono tenuti invece alla conservazione dei documenti in forza delle norme di carattere generale dettate dal Codice civile sulla tenuta della corrispondenza e delle scritture contabili.
Nello specifico, l'art. 2214 c.c. impone di "conservare ordinatamente per ciascun affare" le fatture e le scritture contabili, oltre alla corrispondenza ricevuta e spedita. Analogamente, gli artt. 2220 e 2312 c.c. specificano che le scritture e i documenti dovranno essere conservati per dieci anni dalla data dell'ultima registrazione o dalla cancellazione della società dal registro delle imprese.
Ai soggetti privati si applicano anche tutte le disposizioni relative alla conservazione dei documenti aventi valore fiscale o tributario.
La rilevanza del fenomeno di conservazione digitale si può apprezzare anche in considerazione del fatto che, mentre la conservazione tradizionale dei documenti su supporto analogico richiede e presuppone il mantenimento inalterato nel tempo del supporto e degli eventuali segni apposti sullo stesso, la forma digitale del documento informatico consente di prescindere dalla materialità del supporto, che potrebbe infatti modificarsi nel tempo, tenuto conto della trasformazione ed evoluzione delle risorse materiali. Inoltre, i sistemi di conservazione digitale garantiscono che il documento digitale non si modifichi nel tempo e che il suo contenuto si mantenga integro ed inalterato.

5.2. Il sistema di conservazione digitale dei documenti informatici.

Come si è detto, la conservazione dei documenti informatici consiste in quell'insieme di attività finalizzate a custodire nel tempo gli archivi di documenti informatici.
In tale contesto, l'art. 43 del CAD, così come novellato dal D. Lgs. 217/2017, stabilisce che gli obblighi di conservazione e di esibizione dei documenti si intendono soddisfatti, a tutti gli effetti di legge, a mezzo di documenti informatici, purché le procedure di conservazione degli stessi siano rispettose di quanto stabilito dalle Linee Guida di settore e garantiscano la conformità dei documenti informatici ai relativi originali.
Ci si accorge sin da subito, quindi, che il CAD disciplina solo i principi generali della conservazione digitale, demandando la definizione degli aspetti tecnici alle c.d. "Linee Guida" predisposte dall'AgID (Agenzia per l'Italia Digitale) e successivamente approvate con Decreto del Presidente del Consiglio dei Ministri (DPCM), ai sensi dell'art. 71 CAD.
In attuazione della citata disposizione normativa, con DPCM del 3/12/2013, pubblicato nella Gazzetta ufficiale del 12/03/2014, sono state adottate le "Regole Tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-

bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

Nel solco di quanto stabilito dagli artt. 43 e 44 CAD, l'art. 3 del DPCM del 3/12/2013 definisce il "sistema di conservazione" come quel processo in grado di assicurare, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione dei documenti informatici e dei fascicoli informatici, garantendone caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

Com'è noto, il 12 gennaio 2018 è stato pubblicato in Gazzetta Ufficiale il D. Lgs. 13 dicembre 2017, n. 217, recante modifiche e integrazioni al Codice dell'Amministrazione digitale, in conformità alla delega contenuta in una delle disposizioni della c.d. Legge Madia, la legge di riforma della Pubblica Amministrazione (l. 124/2015).

Tra le novità più significative del recente decreto vi è la modifica di alcune disposizioni sancite in materia di conservazione digitale e, in particolare, delle norme riguardanti, rispettivamente, la conservazione ed esibizione dei documenti informatici, i requisiti per la loro gestione e conservazione e, infine, il valore giuridico della trasmissione.

Prima di analizzare nello specifico quali sono le novità più significative del recente intervento normativo, appare opportuno chiarire quali siano i ruoli delle tre principali figure che vengono in considerazione nel sistema di conservazione: il produttore, l'utente e il responsabile della conservazione.

5.3. Ruoli e responsabilità dei soggetti coinvolti

Ai sensi dell'art. 6 del DPCM del 3/12/2013, si definisce "produttore" del documento informatico quella persona fisica o giuridica, interna e/o esterna al sistema di conservazione, che fornisce all'archivio le informazioni da conservare.

Non sempre il produttore delle informazioni è il diretto autore delle stesse, anzi di norma si tratta proprio di un soggetto diverso da quello che ha formato il documento. Tra i principali compiti e responsabilità del produttore del documento informatico vi è quella di assicurare che i dati e le informazioni contenuto nel documento siano accurate e complete.

In particolare, questa figura ha il compito di gestire i flussi informatici e documentali, sia in entrata che in uscita, garantendone la conservazione nel tempo. Egli produce il c.d. "pacchetto di versamento", ossia quell'aggregazione di documenti e/o fascicoli informatici trasferita, secondo un formato predefinito e concordato, nel sistema di conservazione.

Il soggetto produttore è, dunque, il titolare dell'archivio digitale, ossia il soggetto obbligato per legge alla conservazione del contenuto documentale che produce e/o acquisisce.

Nell'ambito delle Pubbliche Amministrazioni, tale ruolo è ricoperto dal responsabile della gestione documentale.

Il secondo soggetto coinvolto nel sistema di conservazione dei documenti digitali è il "responsabile della conservazione", ossia quel soggetto che si occupa della corretta gestione del sistema di conservazione digitale delle informazioni e documenti, nonché del monitoraggio della corretta funzionalità dello stesso. Tale figura, che potrebbe comunque anche coincidere con il produttore, coopera con quest'ultimo per le attività di versamento dei documenti e si interfaccia con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza, con il responsabile dei sistemi informativi, nonché con il responsabile della gestione documentale, coordinando tutti i processi di dematerializzazione.

Il responsabile della conservazione può, altresì, delegare, sotto la propria responsabilità, un terzo ad eseguire talune o tutte le attività inerenti al processo di conservazione. In questo caso, il responsabile della conservazione avrà una responsabilità a titolo di culpa in eligendo e culpa in vigilando, e dovrà redigere il proprio "Manuale di Conservazione", che conterrà i processi di gestione e formazione dei documenti informatici e del processo di versamento presso il Sistema di Conservazione.

L'AgID (Agenzia per l'Italia Digitale) ha chiarito in una apposita FAQ che, laddove il servizio di conservazione sia affidato in outsourcing a un soggetto privato esterno, il ruolo di responsabile della conservazione può essere svolto esclusivamente da una persona fisica alle dipendenze del soggetto produttore dei documenti da conservare.

Il conservatore esterno designato risponderà quindi al responsabile interno della conservazione e, di conseguenza, anche al soggetto produttore dei documenti informatici.

Nel novero dei soggetti coinvolti nel procedimento di conservazione digitale vi è poi l'"utente", ossia la persona fisica, giuridica o l'ente che si relaziona con il sistema di gestione e/o di conservazione dei documenti informatici, con il fine di ottenere e fruire delle informazioni di suo interesse.

5.4 La formazione di documenti informatici (art. 40 C.A.D.).

Diverse sono le novità introdotte dal D. Lgs. 13 dicembre 2017, n. 217 con riferimento alla materia della conservazione documentale. Si cercherà pertanto di evidenziare, nel presente e nei prossimi paragrafi, quali sono le differenze rispetto alla precedente formulazione del C.A.D. e quali, tra queste, le novità più rilevanti.

In tema di formazione di documenti informatici, si consideri la seguente tabella volta ad evidenziare le novità introdotte con il D.Lg. 217/2017.

D. Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale	
Aggiornamento al D. Lgs. n. 179/2016	Aggiornamento al D. Lgs. n. 217/2017
Art. 40. Formazione di documenti informatici. 1. Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71. 2. (comma abrogato) 3. (comma abrogato) 4. (comma abrogato)	**Art. 40. Formazione di documenti informatici.** 1. Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida. 2. (comma abrogato) 3. (comma abrogato) 4. (comma abrogato)

Da quanto sopra si evince che la formulazione dell'art. 40 CAD rimane pressoché invariata rispetto alla precedente versione normativa, se non per il riferimento alle "Linee Guida" per la formazione dei documenti informatici, le quali, come stabilito dall'art. 71 del C.A.D. dovranno essere adottate dall'AgID (l'Agenzia per l'Italia Digitale) previa consultazione pubblica, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza Unificata (ossia della sede congiunta della Conferenza Stato-Regioni e della Conferenza Stato-Città ed autonomie locali).

5.5 Il protocollo informatico (art. 40-bis C.A.D.).

In tema di protocollo informatico, si consideri la seguente tabella volta ad evidenziare le novità introdotte con il D.Lg. 217/2017.

D. Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale	
Aggiornamento al D. Lgs. n. 179/2016	Aggiornamento al D. Lgs. n. 217/2017
Art. 40-bis. Protocollo informatico. 1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 6-ter, comma 1, 47, commi 1 e 3, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71.	**Art. 40-bis. Protocollo informatico.** 1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida.

Anche in questa ipotesi, si può notare come le differenze nella formulazione della disposizione, rispetto alla precedente versione, siano del tutto marginali. È sicuramente degno di nota il riferimento al "domicilio digitale eletto", che rappresenta una delle novità più rilevanti del nuovo C.A.D.. Tale concetto viene in considerazione, nella fattispecie in esame, come possibile fonte di provenienza delle comunicazioni che sono soggette a "registrazione di protocollo, ai sensi dell'art. 53 del D.P.R. 445/2000", recante il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (c.d. "TUDA").

Dovranno quindi essere oggetto della c.d. "registrazione di protocollo" - registrazione che, come noto, deve riguardare tutti i documenti in entrata e in uscita dall'Ente, ai sensi degli artt. 52 e 53 del TUDA - anche tutte le comunicazioni provenienti o indirizzate al domicilio digitale eletto dal cittadino, ossia, nello specifico, a quell'indirizzo di PEC o altro servizio di recapito certificato equivalente, comunicato alla Pubblica Amministrazione dal cittadino quale proprio domicilio digitale, nonché le istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

5.6 Il sistema pubblico di ricerca documentale (art. 40-ter C.A.D.).

Il D. Lgs. 13 dicembre 2017, n. 217 ha introdotto ex novo l'**art. 40-ter** del C.A.D., dedicato al sistema pubblico di ricerca documentale, a mente del quale: "La Presidenza del Consiglio dei ministri promuove lo sviluppo e la sperimentazione di un sistema volto a facilitare la ricerca dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e di cui all'articolo 40-bis e dei fascicoli dei procedimenti di cui all'articolo 41, nonché a consentirne l'accesso on-line ai soggetti che ne abbiano diritto ai sensi della disciplina vigente".

In particolare, l'anzidetta disposizione assegna alla Presidenza del Consiglio dei Ministri il compito di promuovere lo sviluppo e la sperimentazione di un sistema nazionale di ricerca documentale, finalizzato a facilitare la ricerca e l'accesso on-line da parte dei soggetti che ne abbiano diritto, ai sensi della disciplina vigente, a documenti soggetti ad obblighi di pubblicità legale, trasparenza o a registrazione di protocollo, quali:

- i documenti ricevuti e spediti dalla Pubblica Amministrazione e tutti i documenti informatici (ad esclusione però delle Gazzette Ufficiali, dei notiziari della Pubblica Amministrazione, delle note di ricezione delle circolari e altre disposizioni, dei materiali statistici, degli atti preparatori interni, dei giornali, delle riviste, dei libri, dei materiali pubblicitari, degli inviti a manifestazioni e di tutti i documenti già soggetti a registrazione particolare dell'amministrazione, come previsto dall'art. 53 del D.P.R. 445/2000, cui l'art. 40-ter C.A.D. espressamente rinvia);
- le comunicazioni provenienti o inviate a domicili digitali (eletti ai sensi di quanto previsto all'articolo 3-bis del C.A.D.), nonché le istanze e le dichiarazioni presentate alla Pubblica Amministrazione in conformità alle linee guida, come previsto espressamente dall'art. 40-bis C.A.D.

Tale innovativa piattaforma sarà, altresì, volta a facilitare la ricerca dei fascicoli informatici dei procedimenti amministrativi formati, ai sensi dell'art. 41 C.A.D., dalla Pubblica Amministrazione titolare di un determinato procedimento amministrativo.

5.7 Il procedimento e il fascicolo informatico (art. 41 C.A.D.).

Significative novità sono state introdotte dal D. Lgs. 13 dicembre 2017, n. 217 anche con riferimento al c.d. "fascicolo informatico".

In particolare, tale fascicolo dovrà agevolare la conservazione e il reperimento dei documenti nel nuovo sistema pubblico di ricerca documentale, che dovrà essere istituito come previsto dall'art. 40-ter sopra esaminato.

Secondo quanto previsto dall'art. 41, comma 2-bis, attraverso il nuovo sistema di ricerca documentale, il fascicolo elettronico potrà essere "direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento e dagli interessati".

In altri termini, si dovrebbe giungere a costituire un sistema di livello nazionale all'interno del quale i singoli sistemi delle PA siano in grado di dialogare fra loro attraverso standard di interoperabilità, al fine di permettere ai soggetti a ciò autorizzati la consultazione ed implementazione dei fascicoli procedimentali da parte sia delle P.A. coinvolte che dei cittadini.

Inoltre, la conservazione e l'accessibilità dei documenti amministrativi dovrà essere garantita da un'adeguata gestione in generale del fascicolo informatico, che dovrà quindi avvenire nel rispetto dei principi di corretta gestione documentale e nel rispetto delle regole sulla formazione, gestione, conservazione e trasmissione del documento informatico, comprese quelle in materia di protocollo informatico e quelle relative al sistema pubblico di connettività.

Proprio per rispondere a queste esigenze, il D. Lgs. 13 dicembre 2017, n. 217 ha precisato, all'art. 41, comma 2-ter, lett. e-bis), che il fascicolo informatico così costituito dovrà recare un identificativo che ne consenta l'indicizzazione e la ricerca - rapida ed efficace - attraverso il sistema pubblico di ricerca documentale di cui all'art. 40-ter C.A.D..

Il fascicolo informatico dovrà poi essere formato in modo tale da garantire l'esercizio in via telematica dei diritti di accesso agli atti amministrativi di cui alla L. 7 agosto 1990, n. 241 (recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi") e all'art. 5 del D. Lgs. 14 marzo 2013, n. 33 (in materia di "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni").

A questo proposito, il D. Lgs. 13 dicembre 2017, n. 217 ha precisato, all'art. 41, comma 2-quater, che dovrà essere assicurata all'utente anche l'immediata conoscibilità, sempre per via telematica, dello stato di avanzamento del procedimento amministrativo cui il fascicolo si riferisce, del nominativo e del recapito elettronico del responsabile del procedimento.

Sarà preciso compito dell'AgID quello di predisporre delle Linee Guida idonee al fine di assicurare l'interoperabilità tra i sistemi di gestione dei fascicoli informatici dei procedimenti, i servizi del sistema pubblico di ricerca documentale (di cui all'art. 40-ter del nuovo C.A.D.) e i servizi della Pubblica Amministrazione, ai quali sarà garantito l'accesso in via telematica, in conformità a quanto previsto dall'art. 64-bis del nuovo C.A.D..

5.8 La dematerializzazione dei documenti delle pubbliche amministrazioni (art. 42 C.A.D.).

D. Lgs. 7 marzo 2005, n. 82- Codice dell'Amministrazione Digitale	
Aggiornamento al D. Lgs. n. 179/ 2016	Aggiornamento al D. Lgs. n. 217/2017
Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni. 1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.	**Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni.** 1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle Linee guida.

Come si può notare, in questo caso non sono state introdotte novità particolarmente rilevanti, se non il riferimento alle Linee guida come parametro di riferimento per la sostituzione degli archivi cartacei con archivi informatici, al fine di realizzare la conversione in formato digitale degli atti e documenti cartacei di cui sia necessaria od opportuna la conservazione.

5.9 La conservazione ed esibizione dei documenti (art. 43 C.A.D.).

Come sopra anticipato, l'art. 43 C.A.D., nella nuova formulazione introdotta dal D. Lgs. 13 dicembre 2017, n. 217, stabilisce, al comma 1, che "Gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida". L'intento del legislatore, che emerge chiaramente dalla norma, è quello di promuovere tanto la conservazione quanto l'esibizione dei documenti in formato digitale, come fattore fondamentale per la realizzazione del processo di dematerializzazione: è questa, infatti, la principale novità rispetto alla formulazione precedente della norma, che riguardava invece unicamente la "Riproduzione e conservazione dei documenti".

Tale obiettivo sarà raggiunto, in particolare, nel momento in cui le procedure di conservazione ed esibizione saranno in grado di assicurare la conformità dei documenti digitali a quelli originali, nel rispetto delle Linee Guida di cui al successivo art. 71 del C.A.D. (contenenti le regole tecniche e di indirizzo per l'attuazione del C.A.D. che dovranno essere adottate dall'AgID, sentite le amministrazioni competenti, il Garante per la protezione dei dati personali, e con il parere della Conferenza unificata).

Nel caso particolare in cui il documento informatico sia oggetto di conservazione da parte di una Pubblica Amministrazione, di un gestore di pubblico servizio o di una società a controllo pubblico (ossia dei soggetti individuati dall'art. 2, comma 2 del C.A.D.), viene meno l'obbligo in capo ai cittadini e alle imprese di conservare i suddetti documenti. Infatti, come previsto dall'art. 43, comma 1-bis, costoro potranno in ogni momento richiederne l'accesso al soggetto titolare dell'obbligo di conservazione.

A questo fine, la novella legislativa in esame è intervenuta aggiungendo una seconda parte all'art. 43, comma 1-bis, che ora specifica che "**Le amministrazioni rendono disponibili** a cittadini ed imprese **i predetti documenti attraverso servizi on-line** accessibili previa identificazione con l'identità digitale di cui all'articolo 64 ed integrati con i servizi di cui agli articoli 40-ter e 64-bis".

Per quanto riguarda invece i documenti, le scritture contabili, la corrispondenza ed ogni altro atto già conservato attraverso la sua riproduzione su supporti fotografici, ottici o di altro tipo, questi resteranno validi se ne risulta garantita la conformità agli originali sulla base della disciplina vigente "al momento dell'invio dei singoli documenti nel sistema di conservazione" (art. 43, comma 2 del C.A.D.).

Non si registrano differenze apprezzabili rispetto alla precedente versione normativa con riferimento formulazione dell'art. 43, comma 3 del C.A.D., a mente del quale i documenti informatici di cui sia imposta, per legge o per regolamento, la conservazione, possono essere archiviati anche con modalità cartacee, ma dovranno essere conservati in modo permanente in forma digitale, nel rispetto delle Linee Guida AgID.

Sono in ogni caso fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle Pubbliche Amministrazioni e sugli archivi privati che siano stati dichiarati di notevole interesse storico.

5.10 Gestione e conservazione dei documenti informatici (art. 44 C.A.D.).

Una significativa novità introdotta dal D. Lgs. 13 dicembre 2017, n. 217 in materia di gestione e conservazione dei documenti informatici interessa il comma 1 dell'art. 44 del C.A.D., che, nella versione novellata, così dispone: "Il sistema di gestione informatica dei documenti delle pubbliche

amministrazioni, di cui all'articolo 52 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è organizzato e gestito, anche in modo da assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida".

Per comprendere la portata innovativa della richiamata disposizione normativa, è opportuno ricollegarsi a quanto sopra esposto con riferimento all'art. 40-ter del C.A.D., introdotto ex novo dal D. Lgs. 13 dicembre 2017, n. 217, che promuove la realizzazione del c.d. "sistema pubblico di ricerca documentale", volto a facilitare la ricerca dei documenti soggetti agli obblighi di pubblicità legale, di trasparenza o di registrazione di protocollo.

Sulla base del novellato art. 44, comma 1-bis del C.A.D. è previsto che il sistema di gestione dei documenti informatici delle Pubbliche Amministrazioni sia gestito da un responsabile, che opera d'intesa con il dirigente responsabile dell'ufficio istituito per la transazione digitale (come previsto dall'art. 17 del C.A.D.), con il responsabile del trattamento dei dati personali, se previsto, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni.

Lo scopo delineato dalla norma in esame è proprio quello di definire e gestire quelle che sono le attività che rientrano nelle rispettive sfere di competenza. Almeno una volta all'anno, il responsabile della gestione dei documenti informatici deve poi provvedere a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi, al fine di garantire al meglio il raggiungimento dell'obiettivo di dematerializzazione dei documenti delle pubbliche amministrazioni.

La predisposizione di un tale sistema di gestione dei documenti informatici dovrà poi assicurare, come è stato precisato nella nuova formulazione del comma 1-ter dell'art. 44 C.A.D., che gli oggetti in esso conservati abbiano "caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità", secondo le modalità che dovranno essere indicate nelle Linee Guida adottate dall'AgID.

Il D. Lgs. 13 dicembre 2017, n. 217 ha introdotto ex novo il comma 1-quater dell'art. 44, che così dispone: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il

responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

La conservazione dei documenti informatici potrà quindi essere effettuata all'interno della singola struttura amministrativa o, in alternativa, essere affidata in modo totale o parziale a dei soggetti esterni, siano essi pubblici o privati, a condizione che offrano adeguate garanzie organizzative, tecnologiche e di tutela dei dati personali e che siano accreditati come "conservatori" presso l'AgID, come stabilito a norma dell'art. 34, comma 1-bis, lett. b) del C.A.D..

5.11 Il ruolo dei conservatori accreditati (art. 44-bis C.A.D).

Si consideri ora la seguente tabella volta ad evidenziare le novità introdotte con il D.Lg. 217/2017 sull'argomento.

Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale	
Aggiornamento al D. Lgs. n. 179/2016	Aggiornamento al D. Lgs. n. 217/2017
Art. 44-bis. Conservatori accreditati. 1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso AgID secondo le regole tecniche di cui all'articolo 71. 2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31. 3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.	**Art. 44-bis. Conservatori accreditati.** (Articolo abrogato)

Il “Conservatore accreditato” è quel soggetto, pubblico o privato, che svolge l’attività di conservazione e al quale sia stato riconosciuto dall’AgID il possesso di elevati standard in termini di qualità e di sicurezza del servizio prestato.

L’art. 44-bis del C.A.D., nella formulazione precedente alla novella intervenuta con il D. Lgs. 13 dicembre 2017, n. 217 prevedeva quindi che, al fine di ottenere l’accreditamento presso AgID nel ruolo di Conservatori, fosse necessario dimostrare il possesso di precisi requisiti, attraverso la presentazione di documenti e certificazioni tra cui anche un certificato di conformità ai requisiti tecnici e organizzativi stabiliti dall’AgID, rilasciato da un ente di certificazione accreditato presso un organismo di accreditamento (ACCREDIA in Italia).

La novella è intervenuta sull’argomento, abrogando totalmente l’art. 44-bis e modificando l’art. 29 relativo alla “Qualificazione e accreditamento” dei soggetti che intendono svolgere l’attività di conservatore di documenti informatici, i quali dovranno presentare all’AgID un’apposita domanda di accreditamento, secondo le modalità fissate dalle Linee guida.

A partire dall’entrata in vigore del nuovo C.A.D., quindi, il soggetto che intende chiedere l’accreditamento come conservatore dovrà innanzitutto rispettare le condizioni stabilite dall’art. 24 del Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. In particolare, il richiedente “deve avere **natura giuridica di società di capitali** e deve inoltre disporre di **requisiti di onorabilità, tecnologici e organizzativi**, nonché delle **garanzie assicurative** e di **eventuali certificazioni**, adeguate rispetto al volume dell’attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. I predetti requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei ministri, sentita l’AgID” (art. 29, comma 2 del nuovo C.A.D.).

Con Decreto del Presidente del Consiglio dei Ministri dovranno quindi essere determinati, oltre ai requisiti di cui il richiedente deve essere in possesso al fine di poter ottenere l’accreditamento come conservatore, anche i requisiti e le condizioni per lo svolgimento di tale attività.

5.12 La trasmissione informatica dei documenti (art. 45 C.A.D.).

Strettamente collegata al tema della conservazione dei documenti digitali è la questione della trasmissione informatica dei documenti oggetto di conservazione, di cui agli artt. 45 ss. del C.A.D..

Preme sottolineare, a questo proposito, come la formulazione dell’art. 45 del C.A.D., a seguito della novella normativa di cui al D. Lgs. 13 dicembre 2017, n. 217, sia rimasta pressoché invariata.

La norma disciplina il “Valore giuridico della trasmissione”, ossia dell’invio o ricezione dei documenti informatici da parte della Pubblica Amministrazione, e stabilisce che i documenti trasmessi da chiunque ad una Pubblica Amministrazione, con qualsiasi mezzo telematico o

informatico idoneo ad accertarne la provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
Inoltre, la norma precisa che il documento informatico trasmesso per via telematica si considera comunque spedito - dal mittente - se esso è stato inviato al proprio gestore, e si intende consegnato al destinatario nel momento in cui è reso disponibile all'indirizzo elettronico dichiarato, nella sua casella di posta elettronica messa a disposizione dal gestore.

5.13 Il manuale di conservazione dei documenti informatici.

L'art. 7, comma 1, lettera m) del D.P.C.M. 3 dicembre 2013, recante "Regole tecniche in materia di sistema di conservazione", definisce il manuale di conservazione dei documenti informatici come quello strumento che viene predisposto dal soggetto responsabile della conservazione digitale, il quale ne cura anche l'aggiornamento periodico nel caso in cui si verifichino dei rilevanti mutamenti normativi, organizzativi, procedurali o tecnologici.

Più precisamente, il manuale di conservazione è un documento informatico che, ai sensi dell'art. 8, comma 2 del citato D.P.C.M., deve recare obbligatoriamente una serie di contenuti specificamente descritti dalla norma.

In particolare, esso dovrà indicare:

- i dati dei soggetti che nel tempo hanno ricoperto il ruolo di responsabile del sistema di conservazione, indicando anche se si è trattato di una delega di funzioni;
- la struttura organizzativa, le funzioni, le responsabilità e gli obblighi dei diversi soggetti coinvolti nel processo di conservazione digitale;
- la descrizione delle tipologie di oggetti sottoposti a conservazione, precisando anche i formati gestiti, i metadati da associare alle diverse tipologie di documenti e le eventuali eccezioni;
- la descrizione delle modalità con le quali i c.d. "pacchetti di versamento" vengono presi in carico (precisando anche le modalità di predisposizione del rapporto di versamento);
- la descrizione dei processi di conservazione e trattamento dei pacchetti di archiviazione;
- la modalità in cui si articola il processo di esibizione e di esportazione documentale dal sistema di conservazione, con la produzione del pacchetto di distribuzione;
- la descrizione della struttura del sistema di conservazione (indicando precisamente le sue componenti tecnologiche e fisiche adeguatamente documentate, e le procedure di gestione e di evoluzione delle stesse);

- la descrizione delle procedure di controllo sul funzionamento del sistema di conservazione e sull'integrità degli archivi, con l'indicazione delle soluzioni da adottare in caso di malfunzionamento;
- la descrizione delle procedure per la generazione di duplicati o copie;
- i tempi entro cui le diverse tipologie di documenti devono essere scartate o trasferite in conservazione, se, nel caso delle pubbliche amministrazioni, non sono presenti nel manuale di gestione;
- i casi in cui è previsto l'intervento di un pubblico ufficiale, indicando anche quali sono le modalità e, infine,
- le normative in vigore nei luoghi dove sono conservati i documenti.

Si tratta, dunque, di uno strumento fondamentale perché consente di avere una precisa descrizione del funzionamento del sistema di conservazione dei documenti digitali, fornendo regole e istruzioni per garantire la correttezza del servizio di protocollo informatico, nonché della gestione del flusso documentale e degli archivi.

CAPITOLO 6
TRASPARENZA E ACCESSO

6.1 Trasparenza online ed evoluzione del diritto di accesso

A tre anni dall'emanazione del **d.lgs. 14 marzo 2013, n. 33**, attuativo della delega contenuta nell'art. 1, comma 35, **della legge 6 novembre 2012, n. 190** (Legge Severino) che ha costituito il primo testo organico volto a superare la frammentaria normativa sugli obblighi di pubblicazione e agevolare la standardizzazione delle modalità di pubblicazione, il concetto di trasparenza è stato ampliato dall'art. 2 del **d.lgs. 25 maggio 2016, n. 97** che, nel modificare ed integrare l'art. 1, comma 1 del citato d.lgs. 33/2013, più diffusamente qualifica la trasparenza quale accessibilità totale ai "dati e documenti detenuti dalle pubbliche amministrazioni" e non più solo alle informazioni relative all'organizzazione ed alle sue attività.

Testo originario d.lgs. 33/2013	**Testo novellato a seguito dell'entrata in vigore del d.lgs 97/2016** "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"
Art. 1 (Principio generale di trasparenza) 1. La trasparenza è intesa come accessibilità totale	**Art. 1** (Principio generale di trasparenza) 1. La trasparenza è intesa come accessibilità totale **dei**

delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. 2. La trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino	**dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa** e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. 2. La trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino

Se nella sua prima formulazione, l'art. 1 del d.lgs. 33/2013 in qualche modo abrogava ma di fatto riprendeva la nozione di trasparenza contenuta nell'art. 11, comma 1 del d.lgs. 150/2009 per cui la trasparenza garantiva la conoscibilità dell'organizzazione e delle sue modalità di agire anche attraverso il ricorso ai portali istituzionali, con la modifica intervenuta a seguito dell'emanazione del d.lgs. 97/2016 si è rafforzato il diritto "generale" di accesso ed il diritto alla trasparenza non si limita più soltanto alle "informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" ma si estende anche alla conoscenza di "dati e documenti detenuti dalle pubbliche amministrazioni" con lo scopo anche di "tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa".

Parallelamente alla modifica dell'art. 1, va segnalata anche quella del primo comma dell'art. 2 del d.lgs. 33/2013.

Testo originario d.lgs. 33/2013	**Testo novellato a seguito dell'entrata in vigore del d.lgs 97/2016** "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"
Art. 2 (Oggetto) 1. Le disposizioni del presente decreto individuano gli obblighi di trasparenza concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la sua realizzazione. Ai fini del presente decreto, per pubblicazione si	**Art. 2** (Oggetto) **1. Le disposizioni del presente decreto disciplinano la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione.** Ai fini del presente decreto, per pubblicazione si

intende la pubblicazione, in conformità alle specifiche e alle regole tecniche di cui all'allegato A, nei siti istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione.	intende la pubblicazione, in conformità alle specifiche e alle regole tecniche di cui all'allegato A, nei siti istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione.

Le modifiche all'art. 3 del d.lgs. 33/2013 rafforzano e integrano il diritto di accesso per come declinato dagli artt. 1 e 2.

Testo originario d.lgs. 33/2013	**Testo novellato a seguito dell'entrata in vigore del d.lgs 97/2016** "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"
Art. 3 (Pubblicità e diritto alla conoscibilità) 1. Tutti i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7.	**Art. 3** (Pubblicità e diritto alla conoscibilità) 1. Tutti i documenti, le informazioni e i dati oggetto di **accesso civico, ivi compresi quelli oggetto di pubblicazione** obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7.

Dalla lettura dei modificati art. 1, 2 e 3, è ben chiaro come la riforma intervenuta in attuazione della legge del 7 agosto 2015, n. 124 comporta un ampliamento degli istituti utili al raggiungimento degli scopi della trasparenza. Viene introdotto lo strumento dell'accesso generalizzato che va a completare il modello di trasparenza italiano incentrato, fino alla riforma del 2016, sugli obblighi di pubblicazione on line.

Il principio della trasparenza si eleva quasi a valore di rango costituzionale atteso che lo scopo dichiarato della trasparenza risulta essere la "tutela" dei diritti del cittadino ed il riconoscimento del suo "diritto di informazione", la sua partecipazione all'attività amministrativa e non già soltanto il controllo diffuso sull'utilizzo delle risorse pubbliche e sul perseguimento delle funzioni istituzionali da parte dell'Amministrazione.

A confermare tale orientamento del legislatore, i contenuti degli artt. 27 e 32 della legge costituzionale approvata in seconda votazione a maggioranza assoluta delle Camere il 12 aprile 2016 recante: "Disposizioni per il superamento del bicameralismo paritario, la riduzione del numero dei parlamentari, il contenimento dei costi di funzionamento delle istituzioni, la soppressione del CNEL e la revisione del titolo V della parte II della Costituzione", ma bocciata dal referendum confermativo del 4 dicembre 2016. La legge costituzionale del 2016 modificava, tra gli altri, il comma 2 dell'art. 97 della costituzione (modificato in "I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento, l'imparzialità e la trasparenza dell'amministrazione") e l'art. 118 (nel quale si prevedeva di inserire un secondo comma: "Le

funzioni amministrative sono esercitate in modo da assicurare la semplificazione e la trasparenza dell'azione amministrativa, secondo criteri di efficienza e di responsabilità degli amministratori"). Tale orientamento, tuttavia, non si è concretizzato in modifica della carta costituzionale in quanto la consultazione referendaria tenutasi il 4 dicembre 2016 ha visto prevalere i "no" alla proposta di riforma.

Le riforme di cui si è detto finora sono di fatto il punto di approdo di un'intera stagione legislativa avviata con la "rivoluzione" degli anni '90.

Le quattro leggi Bassanini (L. 59/1997; L. 127/1997; L. 191/1998; L. 50/1999) hanno avviato il cosiddetto "decennio della comunicazione pubblica" supportato parallelamente dalle nuove tecnologie informatiche e telematiche.

Il processo di digitalizzazione della Pubblica Amministrazione italiana è un percorso in parte avviato "incidentalmente" dall'applicazione delle disposizioni normative sulla comunicazione pubblica il cui testo fondamentale è costituito dalla legge 7 giugno 2000, n.150 Disciplina delle attività di informazione e comunicazione delle pubbliche amministrazioni e dal regolamento attuativo contenuto nella Direttiva P.C.M. 21 settembre 2000 sul programma delle iniziative di informazione e comunicazione istituzionale delle amministrazioni dello Stato. La legge, pensata per rendere pubbliche le attività e le funzioni dell'amministrazione, prevedeva, quali strumenti della comunicazione istituzionale delle Pubbliche Amministrazioni, l'Ufficio stampa (art.9), l'Ufficio relazioni con il pubblico – URP (art.8) ed "ogni mezzo di trasmissione idoneo ad assicurare la necessaria diffusione di messaggi, anche attraverso la strumentazione grafico-editoriale, le strutture informatiche, […]" (art.2) che richiamano i moderni mezzi tecnologici di comunicazione come siti web, portali, newsletter.

La legge 150/2000 ha reso alla comunicazione pubblica uno spazio istituzionale ed ha riconosciuto il diritto di accesso anche attraverso il ricorso a forme di concertazione e di partecipazione attiva.

Se guardiamo a tutto il complesso processo di decentramento amministrativo e funzionale avviato nel nostro Paese negli anni 90' e durato 25 anni, riscontreremo come ciò abbia generato nei cittadini una maggiore consapevolezza del diritto di accesso alle informazioni. La legge 142/90 Ordinamento delle autonomie locali all'art. 7, afferma espressamente che "tutti gli atti dell'Amministrazione Comunale e Provinciale sono pubblici, ad eccezione di quelli riservati per espressa indicazione di legge", e statuisce che in apposito Regolamento siano dettate "le norme necessarie per assicurare ai cittadini l'informazione sullo stato degli atti e delle procedure e sull'ordine di esame delle domande, progetti e provvedimenti che comunque li riguardino". Con la legge 241/90 Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi, almeno dal punto di vista formale, la Pubblica Amministrazione orienta la propria azione dall'informazione

al cittadino alla comunicazione bidirezionale. Essa segna il passaggio da un sistema imperniato sulla segretezza ad un sistema che, prendendo le mosse dai principi costituzionali di legalità, imparzialità e buon andamento dell'amministrazione, si basa su trasparenza e pubblicità. L'art. 1 della legge 241/90 fissa quali principi cardine dell'attività amministrativi quelli di pubblicità e trasparenza, riconoscendo tutela ai soggetti privati nell'ambito dei rapporti con la pubblica amministrazione. Tuttavia, il principio che sottende le disposizioni contenute nella legge 241/90 non è ancora quello di un controllo generalizzato sul comportamento della Pubblica Amministrazione.

Gli anni 2000 sono anche gli anni in cui il diritto di cittadinanza, come partecipazione alla vita pubblica e diritto ad essere informati con la massima trasparenza possibile, anche grazie all'impiego delle tecnologie informatiche, è fatto oggetto di diversi interventi normativi dell'Unione. Valga quale riferimento la Carta europea dei diritti dell'uomo nella città (2000) e gli atti della conferenza internazionale promossa nel 2002 dal Consiglio d'Europa sul tema Sviluppo della cittadinanza democratica e di una leadership responsabile a livello locale.

Con l'adozione del d.lgs. 7 marzo 2005, n. 82 – il primo "Codice dell'Amministrazione Digitale" (C.A.D.) - trovano la loro sintesi i principi alla base dell'Amministrazione digitale. Il C.A.D. del 2005 richiama in particolare, quali suoi atti normativi presupposti, la legge 241/90, il d.lgs. 12 febbraio 1993, n. 39 recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, il d.P.R. 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. E tuttavia, il d.lgs. 82/2005, è andato oltre tutto ciò, introducendo interessanti principi e diritti come il diritto all'uso delle tecnologie nei rapporti con le pubbliche amministrazioni; è divenuto il punto di riferimento normativo per la dematerializzazione del documento amministrativo ed, in generale, per lo sviluppo della digitalizzazione della Pubblica Amministrazione. Con il C.A.D. del 2005, l'e-government diviene legge. Tuttavia, a distanza oramai di quasi un ventennio, si può affermare che la Magna Carta dell'amministrazione digitale italiana è tra le norme meno applicate del nostro ordinamento. A partire già dal 2006 e fino al 2017, il codice ha subito diverse modifiche. Un elenco completo degli aggiornamenti e delle modifiche del d.lgs. 82/2005 è disponibile sul sito dell'Agenzia per l'Italia digitale.

La legge 4 marzo 2009, n. 15 Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei Conti individua principi e criteri di delega per il miglioramento complessivo del lavoro e delle prestazioni delle pubbliche amministrazioni (PA), per l'ottimizzazione della produttività del lavoro

pubblico e per una maggiore efficienza e trasparenza delle PA. In attuazione della legge 15/2009, il Governo emana il d.lgs. 150 del 27/10/2009 che reca disposizioni relative alla misurazione, valutazione e trasparenza della performance. Obiettivo dichiarato della riforma è quello di conseguire una migliore organizzazione del lavoro, assicurare il progressivo miglioramento della qualità delle prestazioni erogate al pubblico, ottenere adeguati livelli di produttività del lavoro pubblico e favorire il riconoscimento di meriti e demeriti dei dirigenti pubblici e del personale. L'ambito soggettivo di applicazione di tale norma è costituito dalle Pubbliche amministrazione intese nella definizione di cui all'art. 1, comma 2 del d.lgs. 165/2001 e quindi "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, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Le principali novità della riforma consistono nella necessità che le Pubbliche Amministrazioni individuino i propri obiettivi strategici e operativi che devono essere rilevanti, specifici, misurabili, scanditi temporalmente, condivisi e realizzabili; si dotino di strumenti di misurazione delle performance individuali ed organizzative al fine di valutare il grado di raggiungimento degli obiettivi prefissati; garantiscano il controllo interno ed esterno attraverso la rendicontazione delle performance ed una azione di trasparenza del loro operato anche a garanzia della legalità del loro agire.

Gli attori coinvolti sono, da un lato, i vertici politico-amministrativi, la dirigenza e gli organismi indipendenti di valutazione e dall'altro la Commissione per la valutazione, la trasparenza e l'integrità delle pubbliche amministrazioni (CIVIT) con compiti di indirizzo, di coordinamento e di sovraintendenza che garantiscano un'efficace valutazione ed un adeguato livello di trasparenza delle amministrazioni.

Il d.Lgs. 150/2009 ha evoluto l'idea di "accessibilità totale" (art.11) ad atti, dati e fatti della Pubblica Amministrazione che costituiscono oggetto della pubblica informazione. Con ciò avendo come obiettivo quello di rendere noto come la Pubblica Amministrazione è organizzata e come realizza il suo fine pubblico-istituzionale. In particolare, gli artt. dal 52 al 57, recano disposizioni in merito all'accesso telematico ai dati ed ai documenti delle pubbliche amministrazioni (art.52); alle caratteristiche dei siti della pubbliche amministrazioni (art.53) ed al contenuto degli stessi (art.54);

alla consultazione delle iniziative normative (art. 55); ai dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado (art.56); ai moduli ed ai formulari (art.57).
Con la legge 18 giugno 2009, n. 69 "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile" si ha, dopo quello del 2005, il più importante ed organico intervento normativo in materia di digitalizzazione dei pubblici uffici. La legge 69/2009, ha introdotto il comma 2-ter e 2-quater all'art. 54 del C.A.D. che hanno integrato ulteriormente le disposizioni relative ai contenuti minimi dei siti web delle PA.
Il Ministero per la Pubblica Amministrazione e l'innovazione, il 26 novembre 2009, ha emanato la Direttiva n. 8 con l'obiettivo dichiarato nell'art. 2 di "sviluppare, promuovere e diffondere nelle PA un processo volto a fornire, attraverso i siti web, un accesso diretto, semplificato e qualitativamente valido alle informazioni ed ai servizi resi all'utenza, migliorandone la fruibilità". I siti istituzionali devono garantire accessibilità, intesa come capacità di fornire informazioni fruibili anche da parte di chi presenti disabilità; devono essere usabili, cioè strutturati in modo da garantire una facile reperibilità e fruibilità dei contenuti; devono garantire la trasparenza, intesa come accessibilità totale attraverso la pubblicazione sui siti web istituzionali delle amministrazioni pubbliche delle informazioni relative all'Organizzazione e attraverso la trasparenza devono garantire la partecipazione attiva dei cittadini. Con la riforma C.A.D. introdotta dal d.lgs. 217/2017, il legislatore ha definito nell'art. 53 i principi per la costituzione dei siti istituzionali su reti telematici ed al comma 1-bis ha fatto un esplicito richiamo a quanto ai contenuti del sito "Amministrazione trasparente" di cui all'art. 9 del d.lgs. 33/2013 "Le pubbliche amministrazioni pubblicano, ai sensi dell'articolo 9 del decreto legislativo 14 marzo 2013, n. 33, anche il catalogo dei dati e dei metadati, nonché delle relative banche dati in loro possesso e i regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo di tali dati e metadati, fatti salvi i dati presenti in Anagrafe tributaria". Un'ulteriore richiamo al codice sulla trasparenza lo ritroviamo nell'art. 54 del C.A.D. lì dove si dispone che "I siti delle pubbliche amministrazioni contengono i dati di cui al decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, nonché quelli previsti dalla legislazione vigente".
All'indomani dell'adozione della legge 69/2009, la CIVIT, dovendo rispondere alla sua finalità istituzionale di promuovere la diffusione nelle PA della legalità e della trasparenza, nonché lo sviluppo di interventi a favore della cultura dell'integrità, ha adottato, con la Delibera n. 105/2010 le "Linee Guida per la predisposizione del Programma triennale per la trasparenza e l'integrità". Nella Delibera CIVIT 105/2010 si trova il primo elenco dettagliato dei contenuti minimi che le PA sono obbligate a pubblicare online. La stessa CIVIT, con propria Delibera n. 2 del 5 gennaio 2012,

è ritornata sulla materia con l'emanazione delle "Linee guida per il miglioramento della predisposizione e dell'aggiornamento del Programma triennale per la trasparenza e l'integrità".

Con lo sviluppo del web 2.0, l'e-government apre uno spazio all'idea dell'open government, cioè l'idea di una Pubblica Amministrazione trasparente a tutti i livelli, che consenta al cittadino di realizzare pienamente il principio di partecipazione. L'open government ha configurato la fisionomia di una amministrazione che favorisce la partecipazione attraverso la pubblicità di tutti i suoi atti e le sue decisioni; consente l'accesso a tutti i dati che produce. Tutto ciò non si configura come un nuovo modo di presentarsi dell'organizzazione ma come un nuovo modo di essere della stessa. Presuppone un cambiamento dei processi, del modello gerarchico dell'organizzazione nel suo rapporto con i cittadini che assumono anche un ruolo di controllo. Questo modello, sviluppato soprattutto dall'Amministrazione Obama in seguito all'adozione del Memorandum dell'8.12.2009 che prende il nome di "Open Government Directive", è diventato un riferimento per le Nazioni Unite che nel 2010 hanno raccomandato alle pubbliche amministrazioni di adottare un siffatto schema che, nella sua evoluzione più avanzata vuole condurre alla prassi dell'open data e cioè alla pubblicazione di tutti i dati in possesso dell'amministrazione in formato aperto, fruibile da tutti, senza restrizioni di copyright, brevetti o altre forme di controllo che ne limitino la riproduzione. Lo sviluppo di questi processi coniugato con l'applicazione del web 2.0 ha configurato un nuovo modello di partecipazione attiva.

L'idea di relazione tra pubblico e privato, che mira a superare lo squilibrio storico che esiste tra pubblica amministrazione e cittadino sposa l'attuale concetto di trasparenza che viaggia di pari passo con lo sviluppo dell'amministrazione digitale che consente di trattare i documenti e di gestire i procedimenti con sistemi informatici e con il ricorso all'uso delle tecnologie dell'informazione e della comunicazione. Le ultime revisioni in ordine di tempo del Codice dell'amministrazione digitale introdotte dal d.lgs. 13 dicembre 2017, n. 217, hanno come intento quello di realizzare pienamente la "cittadinanza online". L'art. 12 del C.A.D. rubricato "Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa" prevede che "le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese".

Se con riferimento all'anticorruzione ed alla trasparenza svolge un ruolo centrale l'Autorità Nazionale Anticorruzione, alla realizzazione degli obiettivi dell'Agenda Digitale Italiana sovrintende l'Agenzia per l'Italia Digitale la cui attività è disciplinata dall'art. 14-bis secondo il

quale l'AgID "promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione e nel rapporto tra questa, i cittadini e le imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia".

All'indomani dell'emanazione della legge 6 novembre 2012, n. 190, "legge anticorruzione" gli osservatori hanno constatato come questa norma contenesse due previsioni che di fatto mirano a dare attuazione all'agenda digitale. La prima la si ritrova nell'art. 1, comma 29: "Ogni amministrazione pubblica rende noto, tramite il proprio sito web istituzionale, almeno un indirizzo di posta elettronica certificata cui il cittadino possa rivolgersi per trasmettere istanze […] e ricevere informazioni circa i provvedimenti e i procedimenti amministrativi che lo riguardano". Tale disposizione ribadisce quanto previsto dal C.A.D. che all'art. 47, comma 1, prescrive l'utilizzo della posta elettronica per le comunicazioni tra pubbliche amministrazioni dando indicazioni sulla loro validità ai fini del procedimento amministrativo. Tanto vale anche nei rapporti tra pubbliche amministrazioni e privati ove questi dichiarino il proprio indirizzo.

La seconda previsione è contenuta nel comma 30 del medesimo art. 1 della l. n. 190/2012 e si riferisce all'interazione tra il processo di digitalizzazione ed il diritto di accesso ai documenti amministrativi. Le amministrazioni, "nel rispetto della disciplina del diritto di accesso ai documenti amministrativi […] hanno l'obbligo di rendere accessibili in ogni momento agli interessati, tramite strumenti di identificazione informatica […] le informazioni relative ai provvedimenti e ai procedimenti amministrativi che li riguardano".

La legge n. 190/2012, adottata dall'Italia in risposta ai vincoli internazionali, conteneva come detto anche una delega al governo ai fini dell'adozione del decreto legislativo per il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle pubbliche amministrazioni di cui è promanazione il d.lgs. 33/2013. Già la Convenzione ONU del 2003 contro la corruzione aveva indicato tra gli strumenti di prevenzione il ricorso alla trasparenza amministrativa con riferimento in particolare alla materia di appalti e gestione di risorse finanziarie e aveva invitato gli stati a diffondere informazioni che "permettano agli utenti di ottenere, se del caso, informazioni sull'organizzazione, il funzionamento ed i processi decisionali della pubblica amministrazione". Come previsto nella "legge anticorruzione", il principio della trasparenza costituisce misura fondamentale per le azioni di prevenzione e contrasto anticipato della corruzione. Il portato della norma conferma la scelta di fondo del legislatore di superare il vecchio sistema di accesso ai documenti puntando sul principio di pubblicità favorito dallo sviluppo delle tecnologie. L'amministrazione diviene parte attiva di un processo che garantisce conoscibilità del

proprio essere e del proprio agire. La trasparenza, in questo sistema, diviene, principio cardine e fondamentale dell'organizzazione delle pubbliche amministrazioni e dei loro rapporti con i cittadini. Di fatto, all'esito del percorso di riforma del d.lgs. 33/2013, l'ordinamento ha previsto la coesistenza di tre tipologie di accesso: documentale classico, civico semplice e civico generalizzato. L'uso della parola "accesso" riferita ai tre istituti non deve trarre in inganno facendo immaginare che si tratti del medesimo strumento di tutela, poiché, come si vedrà, i presupposti giuridici e le finalità degli stessi sono sensibilmente differenti. Come l'Autorità Nazionale Anticorruzione (ANAC) ha precisato nelle Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013, approvate, all'indomani della riforma del codice trasparenza, con propria delibera n. 1309 del 28 dicembre 2016, le tre tipologie di accesso che ora convivono nell'ordinamento sono destinate a muoversi su binari differenti.

6.2 Accesso civico semplice

Con la riforma del 2016, l'accesso generalizzato, come detto, non sostituisce l'accesso civico "semplice". Esso rimane circoscritto ai soli atti, documenti e informazioni oggetto di obblighi di pubblicazione e costituisce un rimedio alla mancata osservanza degli obblighi di pubblicazione imposti dalla legge. **L'istituto dell'accesso civico cosiddetto "semplice"** è rinvenibile nell'art. 5 comma 1 del d.lgs. 33/2013 secondo il quale "l'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione". Esso costituisce di fatto il converso dell'obbligo di pubblicazione. Dispone, infatti, che - stante l'elenco tassativamente previsto dalla norma che puntualmente individua i documenti, le informazioni o i dati oggetto di pubblicazione obbligatoria da rendere disponibili sui siti istituzionali - chiunque possa attivare l'accesso civico chiedendo il rispetto dell'adempimento ove questo sia del tutto omesso ovvero risulti lacunoso.

Da un lato l'obbligo della Pubblica Amministrazione di adempiere tenuto riguardo ad una tipizzazione stringente definita dalla norma e dall'altro il diritto di chiunque, indipendentemente dalla sua posizione giuridica rispetto all'oggetto della pubblicazione, di intervenire per spingere l'amministrazione a sanare l'inadempienza.

Si tratta di un istituto che, nelle intenzioni del legislatore, mira a "**rifondare**" il rapporto fiduciario tra cittadini ed amministrazione, promuovere la cultura della legalità utile strumento di prevenzione della corruzione. La relazione di accompagnamento del d.lgs. 33/2013, nel tratteggiare il diritto di

accesso civico come estrinsecazione del principio di trasparenza specifica che "questa nuova forma di accesso mira, da un lato ad alimentare il rapporto di fiducia intercorrente tra la collettività e le pubbliche amministrazioni; dall'altro a promuovere la cultura della legalità, nonché la prevenzione di fenomeni corruttivi. Tale diritto rappresenta un ampliamento del potere di controllo dei cittadini sull'operato delle pubbliche amministrazioni".

A tal riguardo, è il **Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri che, con la circolare n. 2 del 19 luglio del 2013**, chiarisce come lo strumento dell'accesso civico semplice debba essere considerato utile a "vigilare, attraverso il sito web istituzionale, non solo sul corretto adempimento formale degli obblighi di pubblicazione ma soprattutto sulle finalità e le modalità di utilizzo delle risorse pubbliche da parte delle pubbliche amministrazioni e degli altri enti destinatari delle norme" e, per converso, caratterizzandosi come strumento di controllo, valido a produrre "una maggiore responsabilizzazione di coloro che ricoprono ruoli strategici all'interno dell'amministrazione, soprattutto nelle aree più sensibili al rischio corruzione".

Il richiamato art. 5 del d.lgs. 33/2013 individua soggettivamente l'ampia platea dei titolari dell'esercizio del diritto di accesso civico semplice riconoscendo a chiunque il diritto di richiedere dati, documenti e informazioni detenuti dall'amministrazione e che, pur obbligatoriamente ostensibili, non siano stati pubblicati o risultino incompleti. Al contrario, limita l'accesso civico semplice dal punto di vista oggettivo esclusivamente ad oggetti di pubblicazione tassativamente previsti dalla norma.

Dal punto di vista procedurale, l'attivazione del diritto è effettuata da chiunque, senza necessità di motivazione ed esercitata gratuitamente salvo il rimborso dei costi sostenuti in caso di uso di materiale di consumo (carta e stampanti) mentre nulla è dovuto nel caso la fruizione avvenga in forma elettronica. Il comma 3 dell'art. 5 chiarisce, poi, che l'istanza può essere presentata in forma telematica secondo le disposizioni del d.lgs. 82/2005. Tale precisazione risulta, invero, superflua, in quanto il codice per l'amministrazione digitale troverebbe in ogni caso applicazione in tale fattispecie. La previsione normativa chiarisce e dettaglia (art. 65 del codice) le modalità idonee affinché l'istanza possa essere considerata ricevibile dall'amministrazione in quanto validamente atta a fornire una identificazione qualificata dell'istante. Sulle modalità procedurali, si rinvia infra alla trattazione specifica.

Dalla lettura testuale della norma si evince con immediatezza cosa accade nell'ipotesi in cui l'amministrazione riscontri positivamente l'istanza ricevuta: "In caso di accoglimento, l'amministrazione provvede […], nel caso in cui l'istanza riguardi dati, informazioni o documenti oggetto di pubblicazione obbligatoria […], a pubblicare sul sito i dati, le informazioni o i documenti richiesti e a comunicare al richiedente l'avvenuta pubblicazione dello stesso, indicandogli il relativo

collegamento ipertestuale". Non del tutto limpida, invece, appare la procedura da applicarsi nel caso di diniego. L'istanza di accesso civico semplice, infatti, così come chiarisce l'art. 5, comma 3, lettera d), deve essere indirizzata al "responsabile della prevenzione della corruzione e della trasparenza, ove l'istanza abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria". Ma il comma 7 del medesimo richiamato articolo prevede la possibilità, in caso di diniego totale o parziale, di proporre richiesta di riesame al responsabile della prevenzione della corruzione e della trasparenza unificato in un unico soggetto ai sensi dell'art. 1, comma 7 della legge 190/2012, come modificato dal d.lgs. 97/2016. È del tutto evidente che, se tale possibilità di ricorso ad un soggetto dotato di potere di riesame è applicabile nel caso dell'esercizio del diritto di accesso civico generalizzato per le ragioni di cui si dirà più innanzi in occasione della specifica trattazione di tale istituto, di converso non sembra azionabile nel caso dell'accesso civico semplice in quanto l'istanza è già in prima battuta avanzata all'indirizzo del responsabile della prevenzione della corruzione e della trasparenza. Per superare questa inconciliabilità delle disposizioni normative, quindi, è necessario identificare il responsabile della prevenzione della corruzione e della trasparenza esclusivamente come il soggetto deputato a ricevere l'istanza dell'interessato ed a darne riscontro a conclusione del procedimento mentre quest'ultimo, nella fase istruttoria, non può che essere condotto dall'Ufficio competente per materia. Solo nell'ipotesi di una procedimentalizzazione così concepita, resta di fatto in capo al responsabile per la prevenzione della corruzione e della trasparenza il potere di riesame che garantisce anche per il diritto di accesso semplice la possibilità di non azionare immediatamente una tutela sul piano giurisdizionale.

Inoltre, la previsione normativa secondo la quale la richiesta di accesso civico semplice deve essere inviata al responsabile per la prevenzione della corruzione e della trasparenza, trova la sua giustificazione nel fatto che la sezione "Amministrazione trasparente" è direttamente sotto il suo controllo e dove questi constati che si è verificato effettivamente un inadempimento degli obblighi di pubblicazione, dovrà attivare le procedure di segnalazione previste dall'art. 43 del codice della trasparenza.

Il procedimento di accesso attivato può concludersi con un rigetto ove l'amministrazione constati che la richiesta abbia ad oggetto la pretesa della pubblicazione di atti, documenti e informazioni non soggette ad obbligo di ostensione ai sensi del d.lgs. 33/2013; ovvero con l'accertamento di quanto segnalato e la conseguente pubblicazione in caso di effettiva inadempienza. In ogni caso, il procedimento si conclude con un provvedimento espresso di rigetto o di accoglimento; in quest'ultimo caso l'amministrazione dà conto anche dell'avvenuta pubblicazione con dettaglio del collegamento ipertestuale a cui riferirsi.

6.2.1 Accesso civico generalizzato

Una delle novità più impostanti della riforma del 2016 al codice sulla trasparenza è costituita dall'introduzione nel nostro ordinamento dell'istituto dell'accesso civico generalizzato. La revisione del d.lgs. 33/2013 ad opera del d.lgs. 97/2016 è l'effetto dell'applicazione della **legge delega 7 agosto 2015, n. 124** (cosiddetta legge Madia).

L'art. 7, primo comma, lettera h) della legge 124/2015, tenendo fermi gli obblighi di pubblicazione, riconosce la "libertà di informazione attraverso il diritto di accesso, anche per via telematica, di chiunque, indipendentemente dalla titolarità di situazioni giuridicamente rilevanti, ai dati e ai documenti detenuti dalle pubbliche amministrazioni, salvi i casi di segreto o di divieto di divulgazione previsti dall'ordinamento e nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati, al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche". Come già detto, una ridefinizione del principio di trasparenza, come strumento di tutela dei diritti dei cittadini e di promozione della partecipazione degli interessati all'attività amministrativa.

Nella nuova formulazione l'art. 5 mostra analogia di finalità tra accesso civico semplice ed accesso generalizzato ma differenti modalità di perseguimento delle stesse.

Testo originario d.lgs. 33/2013	**Testo novellato a seguito dell'entrata in vigore del d.lgs 97/2016** "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"
Art. 5 (Accesso civico) 1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione. 2. La richiesta di accesso civico non è sottoposta ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente non deve essere motivata, è gratuita e va presentata al responsabile della trasparenza dell'amministrazione obbligata alla pubblicazione di cui al comma 1, che si pronuncia sulla stessa. 3. L'amministrazione, entro trenta giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente,	**Art. 5** (Accesso civico a dati e documenti) 1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione. 2. Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis. 3. L'esercizio del diritto di cui ai commi 1 e 2 non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. L'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti e non richiede motivazione.

l'amministrazione indica al richiedente il relativo collegamento ipertestuale.	

La lettura del comma 2 dell'art. 5 mostra chiaramente come per l'esercizio dell'istituto dell'accesso generalizzato si è tenuto fermo l'ambito soggettivo che non subisce alcuna limitazione riguardo alla legittimazione mentre si è ampliato l'ambito oggettivo di applicazione del medesimo. Sicché, il diritto di accesso semplice e quello generalizzato possono entrambi essere attivati "da chiunque"; inoltre, in ambedue l'istanza non necessita di una motivazione. Nel caso dell'accesso civico semplice la motivazione non è richiesta poiché l'amministrazione rispondendo all'istanza soddisfa un obbligo ad adempiere già definito dalla norma; nel caso dell'accesso generalizzato la motivazione è espressamente non richiesta e come tale non può costituire elemento necessario per la procedibilità da parte dell'amministrazione. La motivazione, quindi, diviene elemento opzionale che resta facoltà nella facoltà del richiedente specificarla o meno a supporto della propria istanza. Tuttavia, tenuto conto dell'attività di bilanciamento che l'amministrazione dovrà effettuare tra le ragioni dell'accoglimento o del diniego all'accesso, essa potrebbe avere un suo peso.

Il comma 3 dell'articolo di che trattasi stabilisce che "l'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti". Su questo punto ampio è stato il dibattito sia prima che dopo il varo della riforma. Mentre nel caso dell'accesso civico semplice, è alla portata di chiunque identificare gli oggetti della richiesta coincidendo questi con quelli tipizzati dalla norma, nel caso dell'accesso di che trattasi in questa sede tale identificazione potrebbe non essere agevole presupponendo la lettera della disposizione normativa che il richiedente sia già a conoscenza di quanto detenuto dall'amministrazione. È ipotizzabile, quindi, che l'amministrazione destinataria dell'istanza di accesso la rigetti in caso di mancanza di tale chiara identificazione? A tal proposito si richiama qui la **circolare n. 2 del 30 maggio 2017 del Ministero per la semplificazione e la pubblica amministrazione di "Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)** emanata con l'intento, relativamente al nuovo istituto di accesso, di fornire alle amministrazioni "chiarimenti operativi, riguardanti il rapporto con i cittadini e la dimensione organizzativa e procedurale interna". In base all'art. 5, c. 3, d.lgs. n. 33 del 2013 – precisa la citata circolare - è sufficiente che la richiesta "identifichi" i dati o i documenti che si vogliono ottenere. Nel valutare l'adeguatezza di tale identificazione, le pubbliche amministrazioni devono tener conto della difficoltà che il richiedente può incontrare nell'individuare con precisione i dati o i documenti di suo interesse. Al punto 11.3 del parere reso, nell'adunanza del 18 febbraio 2016, dalla sezione consultiva per gli atti normativi del Consiglio di Stato (parere sullo schema di decreto legislativo recante "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione,

pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche), il Consiglio ha rappresentato al legislatore come sarebbe "incongruo" che l'istanza di accesso civico "considerati i suoi presupposti e le sue finalità" debba essere "già in grado di identificare "chiaramente" i dati, le informazioni o i documenti richiesti, contravvenendosi allo scopo per cui il nuovo istituto è oggetto di implementazione". Il Consiglio di Stato, in tale sede, ha quindi suggerito al legislatore di espungere tale avverbio semmai sostituendolo con la locuzione "natura ed oggetto". Il legislatore, tuttavia, in sede di approvazione definitiva del decreto, ha ritenuto di accogliere il suggerimento del Consiglio eliminando l'avverbio "chiaramente" ma non lo ha sostituito con la locuzione proposta. Stante ciò, con la circolare n. 2/2017 citata, il Ministero ha ritenuto necessario intervenire raccomandando alle amministrazioni di "assistere il richiedente al fine di giungere a una adeguata definizione dell'oggetto della domanda" lì dove questa sia "formulata in termini talmente vaghi da non consentire di identificare l'oggetto della richiesta (c.d. richiesta generica) o volta ad accertare il possesso di dati o documenti da parte dell'amministrazione (c.d. richiesta esplorativa)".

Nell'ipotesi di richiesta generica o meramente esplorativa, nelle citate **linee guida ANAC di cui alla delibera n. 1309/2016** si ammette la possibilità di dichiarare la domanda inammissibile, ma si chiarisce che, prima di dichiarare l'inammissibilità, "l'amministrazione destinataria della domanda dovrebbe chiedere di precisare l'oggetto della richiesta". Pertanto, questa ipotesi di inammissibilità deve essere intesa in senso restrittivo: l'amministrazione dovrebbe ritenere inammissibile una richiesta formulata in termini generici o meramente esplorativi soltanto quando abbia invitato (per iscritto) il richiedente a ridefinire l'oggetto della domanda o a indicare gli elementi sufficienti per consentire l'identificazione dei dati o documenti di suo interesse, e il richiedente non abbia fornito i chiarimenti richiesti (Ministero per la semplificazione e la pubblica amministrazione, circolare n. 2/2017 FOIA). Devono essere ritenute validamente formulate e quindi ricevibili le richiesta di accesso generalizzato quando queste, pur non individuando il provvedimento che li contiene, identificano i dati di cui richiedono la conoscenza. In questo caso, l'amministrazione, in condizione di fare una ricognizione documentale al suo interno, persegue la via più idonea a soddisfare la richiesta.

Ricorre nel comma 2 dell'art. 5 in trattazione, la specifica secondo la quale "chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni". Viceversa, nel comma 1, più propriamente riconducibile all'istituto dell'accesso civico semplice, si parla di "obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati". Come si noterà, nel comma 1, che disciplina l'accesso civico semplice si parla

di documenti informazioni o dati; nel caso del comma 2, così come del comma 4 e 6, ci si riferisce esclusivamente a dati e documenti. È evidente, in un caso e nell'altro, che non è richiesta all'amministrazione alcuna attività di reperimento di dati, documenti o informazioni di cui non sia già in possesso, tantomeno vige qui la preclusione di acconsentire l'accesso ad informazioni e dati che non abbiano la forma del provvedimento. Tuttavia, è significativa la differente formulazione della norma tra i diversi commi dell'art. 5. Nel caso dell'accesso civico generalizzato, l'istanza deve limitarsi alla richiesta di dati e documenti in possesso dell'amministrazione - indipendentemente da chi li abbia prodotti o trasmessi alla stessa - senza la pretesa di alcuna rielaborazione. Sicché questa circostanza costituirà un limite alla richiesta di accesso. Nell'ipotesi di accesso civico semplice le amministrazioni, al fine di adempiere correttamente all'obbligo di pubblicazione, sono spesso tenute alla rielaborazione di dati e informazioni anche nei casi in cui questi siano già contenuti in propri provvedimenti.

Una trattazione specifica è stata dedicata alla cosiddetta "Pubblicazione proattiva". Nella citata Circolare n. 2/2017 FOIA "per accrescere la fruibilità delle informazioni di interesse generale e l'efficienza nella gestione delle domande, si raccomanda alle amministrazioni di valorizzare la possibilità di pubblicare informazioni anche diverse da quelle oggetto di pubblicazione obbligatoria, fermo restando il rispetto delle esclusioni e dei limiti previsti dall'art. 5-bis, c. 1-3, del d.lgs. n. 33/2013. In particolare, la pubblicazione proattiva sui siti istituzionali delle amministrazioni è fortemente auspicabile quando si tratti di informazioni di interesse generale o che siano oggetto di richieste ricorrenti: ad esempio, quando si tratti di dati o documenti richiesti, nell'arco di un anno, più di tre volte da soggetti diversi. Per gli stessi motivi, le pubbliche amministrazioni sono invitate a valorizzare il dialogo con le comunità di utenti dei social media (Facebook, Twitter, ecc.). I richiedenti spesso rendono pubbliche su questi mezzi di comunicazione le domande di accesso generalizzato da essi presentate. In questi casi, e comunque quando si tratti di informazioni di interesse generale, è opportuno che anche le amministrazioni utilizzino i medesimi canali a fini di comunicazione".

6.3 Procedimento per l'accesso e controinteressati

Il più volte citato art. 5 dettaglia il processo gestionale per soddisfare l'istanza di accesso. A tal proposito, la più volte citata circolare n. 2/2017, emanata dal Ministero per la semplificazione e la pubblica amministrazione, ha offerto alle Amministrazioni ulteriori suggerimenti procedurali da adottare al fine di agevolare in particolare l'esercizio del diritto di accesso generalizzato da parte degli utenti.

Come già anticipato, nulla quaestio circa le modalità di trasmissione dell'istanza di accesso. Il comma 3 dell'art. 5 del d.lgs. 33/2013 fa un rimando esplicito alle modalità previste dal C.A.D. Tuttavia, anche se tale modalità non è espressamente richiamata dalla lettera della norma, resta fermo che l'istanza può essere presentata ai sensi dell'art. 38, commi 1 e 3, del d.P.R. 28 dicembre 2000, n. 445 anche a mezzo posta, fax o direttamente presso gli uffici indicati dal medesimo art. 5, comma 3, del d.lgs. n. 33/2013 e che laddove la richiesta di accesso non sia sottoscritta dall'interessato in presenza del dipendente addetto, la stessa debba essere sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore che va inserita nel fascicolo.

Secondo quanto dispone la circolare ministeriale n. 2/2017 sul FOIA, le Amministrazione dovrebbero predisporre e rendere disponibile, nella pagina su "Accesso generalizzato" della sezione "Amministrazione trasparente" e con link nella home page, "informazioni generali su:

- la procedura da seguire per presentare una domanda di accesso generalizzato;
- i rimedi disponibili (procedura di riesame e ricorso in via giurisdizionale), ai sensi dell'art. 5, c. 7, d.lgs. n. 33/2013, in caso di mancata risposta dell'amministrazione entro il termine di conclusione del procedimento o in caso di rifiuto parziale o totale dell'accesso;
- il nome e i contatti dell'ufficio che si occupa di ricevere le domande di accesso;
- due indirizzi di posta elettronica dedicati alla presentazione delle domande: un indirizzo di posta elettronica certificata (PEC) collegato al sistema di protocollo; un indirizzo di posta ordinaria, con il quale deve essere sempre consentito l'invio di domande da parte dei richiedenti che non dispongano a loro volta di un indirizzo PEC per l'invio;
- due moduli standard utilizzabili, rispettivamente, per proporre: una domanda di accesso generalizzato; una domanda di riesame. In ogni caso, l'uso di un formato o modulo diverso da quello reso disponibile online sul sito istituzionale dell'amministrazione non può comportare l'inammissibilità o il rifiuto della richiesta".

Nella medesima circolare, il Ministero suggerisce alle amministrazioni alcune soluzioni tecniche per agevolare l'esercizio del diritto di accesso generalizzato da parte dei cittadini e, al contempo, "gestire in modo efficiente le richieste di accesso, la principale è la realizzazione di un registro degli accessi, come indicato anche nelle Linee guida A.N.AC. (delibera n. 1309/2016). Il registro dovrebbe contenere l'elenco delle richieste e il relativo esito, essere pubblico e perseguire una pluralità di scopi: - semplificare la gestione delle richieste e le connesse attività istruttorie; - favorire l'armonizzazione delle decisioni su richieste di accesso identiche o simili; - agevolare i cittadini nella consultazione delle richieste già presentate; - monitorare l'andamento delle richieste di accesso e la trattazione delle stesse. […] Ai fini della pubblicazione periodica del registro

(preferibilmente con cadenza trimestrale), le amministrazioni potrebbero ricavare i dati rilevanti attraverso estrazioni periodiche dai sistemi di protocollo informatico. […]. L'obiettivo finale è la realizzazione di un registro degli accessi che consenta di "tracciare" tutte le domande e la relativa trattazione in modalità automatizzata, e renda disponibili ai cittadini gli elementi conoscitivi rilevanti".

Come detto, lo stesso comma 3 individua anche gli uffici a cui è possibile indirizzare l'istanza di accesso generalizzato. Questa può essere inviata a) all'ufficio che detiene i dati, le informazioni o i documenti;

b) all'Ufficio relazioni con il pubblico;

c) ad altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale. La scelta dell'ufficio a cui indirizzare la richiesta dipende, ovviamente, dal livello di conoscenza dell'organizzazione e dal grado di consapevolezza del tipo di informazioni richieste. Il ricorso all'Ufficio relazioni con il pubblico è tipicamente previsto per una fase di prima ricognizione ed orientamento del richiedente, lì dove questi non abbia piena contezza delle informazioni da richiedere o del fatto che queste siano effettivamente in possesso dell'amministrazione interpellata. La possibilità per l'amministrazione di individuare un ufficio ad hoc destinatario delle istanze, viene incontro ad una esigenza organizzativa e potrebbe, nella prassi applicativa, risolvere le incongruenze della norma per gli aspetti relativi al riesame in caso di diniego all'istanza di accesso civico semplice. La norma, quindi, configura la possibilità di procedimentalizzare sia l'accesso civico semplice che quello generalizzato prevedendo che, indipendentemente dall'ufficio ricevente l'istanza, su questa decida, dopo aver condotto l'istruttoria, un ufficio a ciò specificamente deputato. Una siffatta organizzazione nell'esercizio di tale funzione, costituisce una garanzia per l'amministrazione di coerenza nel trattare e riscontrare le richieste di accesso, riservando al Responsabile per la prevenzione della corruzione e della trasparenza l'attività di riesame, ove richiesta, o il potere di sostituzione in caso di inadempimento.

Nel caso in cui sia palese che la domanda è stata erroneamente indirizzata a un'amministrazione diversa da quella che detiene i dati o documenti richiesti, l'ufficio ricevente deve inoltrare tempestivamente la domanda all'amministrazione competente e darne comunicazione al richiedente, specificando che il termine di conclusione del procedimento decorre dalla data di ricevimento della richiesta da parte dell'ufficio competente (circolare n. 2/2017, Ministero per la semplificazione e la pubblica amministrazione).

Per quel che attiene alla ricevibilità della richiesta, quando questa viene sottoposta a valutazione da parte dell'amministrazione, si deve tenere conto del fatto che, in questo quadro normativo, il legislatore ha inteso dare tutela preferenziale all'interesse a conoscere che la richiesta mira a

soddisfare. Sicché, con riferimento al piano procedurale, le amministrazioni non possono opporre motivi formali o procedurali per l'ammissibilità delle domande di accesso generalizzato. Torna, qui quanto già argomentato circa il dovere dell'amministrazione di "assistere" il richiedente al fine di giungere, ove possibile, alla soddisfazione della pretesa di conoscere.

Per assistere il richiedente e per effettuare materialmente il riscontro, è di tutta evidenza che l'amministrazione deve poter identificare in modo inequivocabile il soggetto che avanza la richiesta di accesso. Sia quando l'amministrazione abbia necessità di avviare un dialogo cooperativo sia nel momento in cui questa debba dare seguito, accogliendola, alla richiesta di fornire dati e documenti richiesti, è indispensabile che il richiedente sia identificato, pena la irricevibilità della richiesta. E tuttavia, prima di dichiarare irricevibile la richiesta, l'amministrazione dovrà sollecitare il richiedente, dando indicazioni puntuali sulle modalità da seguire, affinché si identifichi. L'identificazione del richiedente rileva anche in fase di valutazione sul merito della richiesta in quanto l'amministrazione deve poter stimare se la domanda non rientri in realtà in una serialità di domande identiche, massive o vessatorie, provenendo sempre dal medesimo soggetto ed in tempi ravvicinati. Del resto, come rilevato dalla giurisprudenza **(TAR Lombardia, Milano, sez. III, 11 ottobre 2017, n. 1951**), nel dare seguito all'istanza di accesso civico generalizzato, l'amministrazione non può non tenere conto della finalità che l'istituto intende perseguire. Poiché è pacifico e dichiarato che l'istituto in parola costituisce uno strumento di tutela dei diritti dei cittadini e di promozione della partecipazione degli interessati all'attività amministrativa, utilizzare il diritto di accesso generalizzato in modo tale da intralciare l'attività amministrativa compromettendone il buon funzionamento, significa tradire la sua primigenia finalità. L'esercizio di tale diritto deve essere effettuato secondo buona fede e senza che si configuri un "abuso del diritto" medesimo. Per la giurisprudenza non è accettabile per l'amministrazione dare seguito a richieste irragionevoli e sovrabbondanti. Tale principio è ribadito nelle citate Linee guida ANAC di cui alla Delibera n. 1309/2016: "nei casi particolari in cui venga presentata una domanda di accesso per un numero manifestamente irragionevole di documenti, imponendo così un carico di lavoro tale da paralizzare, in modo molto sostanziale, il buon funzionamento dell'amministrazione, la stessa può ponderare, da un lato, l'interesse dell'accesso del pubblico ai documenti e, dall'altro, il carico di lavoro che ne deriverebbe, al fine di salvaguardare, in questi casi particolari e di stretta interpretazione, l'interesse ad un buon andamento dell'amministrazione".

Nel caso dell'acceso civico semplice, risulta, invece attenuata, per ragioni intuitive, la necessità dell'identificazione del richiedente trattandosi in quel caso di obbligo di facere (pubblicare) a cui l'amministrazione "deve" dare seguito.

Una volta che l'amministrazione abbia accolto la richiesta di accesso, il procedimento deve esitare entro trenta giorni con l'emissione di un provvedimento espresso e motivato. Qualora l'amministrazione individui dei controinteressati all'accesso, questi saranno coinvolti nel procedimento ricevendo copia dell'istanza ed avranno dieci giorni per esprimere in merito il proprio consenso. In tal caso, il termine per l'adozione del provvedimento finale motivato ed espresso sarà pari a quarantacinque giorni. Quando il procedimento si conclude con l'accoglimento e senza che vi siano state opposizioni da parte degli eventuali controinteressati, il provvedimento nonché i documenti ed i dati oggetto della richiesta devono essere immediatamente inoltrati al richiedente, preferibilmente, in modo contestuale. Ai controinteressati sarà inviato il solo provvedimento di accoglimento dell'istanza di accesso. Nell'ipotesi in cui gli eventuali controinteressati facciano una qualche opposizione alla richiesta di accesso, il provvedimento di accoglimento non potrà dare seguito al rilascio dei documenti e dati richiesti prima che siano trascorsi quindici giorni dalla notizia ai controinteressati dell'avvenuto accoglimento e ciò al fine di consentire loro di attivare le tutele previste dal comma 9 dell'art. 5 del d.lgs. 33/2013, secondo le modalità normate dai comma 7 e 8 del medesimo articolo.

Una questione di non poco conto sulla quale, a dirla tutta, non si dibatte dall'introduzione nell'ordinamento dell'accesso generalizzato ma che offre spunti di confronto fin dalla nascita dell'istituto dell'accesso documentale ai sensi della l. 241/90, è quella relativa all'individuazione di coloro i quali devono, nel caso concreto, essere considerati "controinteressati". L'art. 3 del d.P.R. 184/2006 ha di fatto introdotto, nel procedimento di accesso documentale, il subprocedimento di notifica dell'istanza al controinteressato. Nel caso dell'accesso documentale classico, viene in soccorso l'art. 22, comma 1, lettera c) della l.241/90 che individua i controinteressati in "tutti i soggetti individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza". Nel caso dell'accesso generalizzato, i controinteressati sono individuati dall'art. 5-bis, comma 2 del d.lgs. 33/2013 secondo il quale: "L'accesso di cui all'articolo 5, comma 2, è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati: a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia; b) la libertà e la segretezza della corrispondenza; c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali". Qui ci si riferisce, evidentemente, ai controinteressati all'accesso, procedimento autonomo e speciale rispetto ad altri procedimenti. Non si tratta di quei soggetti che potrebbero trarre un pregiudizio dal contenuto di un provvedimento finale a conclusione di qualsivoglia procedimento amministrativo. Si tratta di soggetti che subirebbero un pregiudizio alla riservatezza dalla presa visione o dalla

estrazione di copia da parte di terzi dei documenti oggetto di accesso. Il pregiudizio che può derivare a terzi dall'esame di documenti in seguito ad accesso generalizzato è limitato al diritto alla riservatezza, tutelato dalla legge.

L'art. 5 del d.lgs. 33/2013 prevede che, nel caso del coinvolgimento dei controinteressati, possa essere chiamato in causa il Garante della protezione dei dati personali che, in veste consultiva, in occasione delle procedure di ricorso interno nel procedimento di accesso, dà il proprio contributo ove si discuta del bilanciamento tra trasparenza e protezione dei dati personali. In tale procedimento, il Garante ha la funzione di contribuire alla decisione di limitare il diritto di accesso di concerto con l'amministrazione.

6.4 Rapporto tra accesso civico e accesso documentale classico

L'introduzione nell'ordinamento dell'istituto dell'accesso civico generalizzato apparentemente in opposizione all'acceso documentale ex l. 241/90, ha procurato un certo disorientamento delle amministrazioni che, nell'immediatezza dell'applicazione della nuova norma, hanno manifestato non poche incertezze interpretative ed applicative.

Uno dei principi cardine della l. 241/90 è quello di trasparenza e pubblicità contenuto nell'art. 1. Una trasparenza che si concretizza attraverso: 1) l'esercizio del diritto di accesso inteso quale diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi - intendendo per interessati tutti i soggetti privati che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso, in una stretta correlazione tra il documento amministrativo oggetto del diritto di accesso e uno specifico interesse del soggetto richiedente; 2) l'obbligo di motivazione dei provvedimenti amministrativi, stabilito dall'art. 3 l. 241/90; 3) la partecipazione dei privati al procedimento che li coinvolge secondo gli artt. 7-13 l. 241/90.

L'esercizio dell'accesso civico generalizzato, come già detto, non è sottoposto ad alcuna limitazione dal punto di vista della legittimazione soggettiva del richiedente.

In quanto detto, è immediatamente rinvenibile una differenza sostanziale tra i due istituti: il diritto di accesso generalizzato, configurandosi come volto a consentire un controllo diffuso sull'agire dell'amministrazione, non pone alcun limite alla legittimazione soggettiva del richiedente accesso; il diritto di accesso documentale, per espressa e perentoria lettera della norma non utilizzabile per sottoporre l'amministrazione ad un controllo generalizzato, è azionabile esclusivamente dagli interessati per come definiti poc'anzi. Inoltre, nel caso del ricorso all'esercizio del diritto di accesso documentale classico, l'interessato ha la facoltà di intervenire nel procedimento che lo interessa

vedendosi riconoscere una partecipazione attiva che nel caso dell'accesso conoscitivo generalizzato non è prevista.

La richiesta di accesso classico, a differenza di quello generalizzato, richiede la motivazione specificando, quindi, l'interesse connesso all'oggetto della richiesta. Nel caso della richiesta di accesso generalizzato, per i presupposti sottesi a tale esercizio, la motivazione non è obbligatoria.

Il procedimento di accesso documentale classico si conclude entro trenta giorni dal ricevimento dell'istanza. In caso di silenzio si intende rifiuto; nel caso di provvedimento di diniego, differimento o limitazione il provvedimento contiene la motivazione. Il termine dei trenta giorni è sospeso nel caso in cui l'amministrazione avvia una interlocuzione con il soggetto che ha avanzato richiesta quando questa risulti incompleta o irregolare.

La richiesta di accesso generalizzato, invece, deve sempre concludersi con un provvedimento espresso e motivato trattandosi di un diritto funzionale ad una sfera di libertà. Ed in caso di mancata ottemperanza, lì dove l'amministrazione resti in silenzio, tale silenzio non si configura come silenzio-rifiuto ma piuttosto come silenzio-inadempimento con le responsabilità che da ciò derivano.

Va fatto qui un cenno circa le disposizioni contenute nell'art. 41 del C.A.D., secondo il quale (comma 1) le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione. "L'amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati" (comma 2).

Ai fini della disciplina dell'accesso, rileva quanto previsto dall'art. 41, comma 2-quater secondo il quale "Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento".

6.5 Banche dati pubbliche

L'art. 2, comma e del d.lgs. 33/2013 identifica il concetto di pubblicazione con l'obbligo per le amministrazioni di mettere a disposizione, tramite i propri siti istituzionali, di documenti informazioni e dati concernenti le loro attività e la loro organizzazione. L'accesso ai siti deve essere

garantito senza alcuna limitazione. In questa attività, che non ha elementi di discrezionalità, l'amministrazione è parte attiva.

La legge delega n. 124/2015, all'art. 7, comma 1 dà mandato al governo di adottare provvedimenti di "c) riduzione e concentrazione degli oneri gravanti in capo alle amministrazioni pubbliche, ferme restando le previsioni in materia di verifica, controllo e sanzioni; d)...; e) razionalizzazione e precisazione degli obblighi di pubblicazione nel sito istituzionale, ai fini di eliminare le duplicazioni e di consentire che tali obblighi siano assolti attraverso la pubblicità totale o parziale di banche dati detenute da pubbliche amministrazioni; […] semplificazione delle procedure di iscrizione negli elenchi dei fornitori, prestatori di servizi ed esecutori di lavori".

Con le modifiche intervenute al d.lgs. 33/2013 da parte del decreto di riforma del 2016, il legislatore ha di fatto sgravato privati ed amministrazioni di un certo numero di obblighi di pubblicazione, escludendone molti dall'ostensione on line. Si è ritenuto che l'introduzione dell'accesso civico generalizzato possa fare da contraltare a questa riduzione di obblighi di pubblicazione consentendo, di converso, a chiunque l'accesso diffuso ad un numero ancora maggiore di informazioni rispetto a quanto avveniva prima della riforma. Tuttavia, non si può non constatare che il ridimensionamento degli obblighi di pubblicazione di dati, informazioni e atti ha di fatto comportato una maggiore "burocratizzazione" della trasparenza che si sottomette ad una azione propulsiva degli interessati attraverso una specifica istanza.

Per l'effetto dell'introduzione, inoltre, dell'art. 9-bis al d.lgs. 33/2013 è stata prevista una forma di pubblicità cosiddetta "sostitutiva". Tutti quei dati che sono soggetti a pubblicazione obbligatoria nei siti "Amministrazione trasparente" e che sono contestualmente obbligatoriamente conferiti in banche dati centralizzate di altre pubbliche amministrazioni possono intendersi pubblicati con il semplice inserimento del collegamento ipertestuale sul sito istituzionale dell'amministrazione che rimanda al sito della banca dati centralizzata. La responsabilità della correttezza, completezza e aggiornamento del dato resta in capo all'amministrazione che lo ha prodotto e che lo conferisce alla banca dati centralizzata, dell'assolvimento dell'obbligo di pubblicazione risponde l'amministrazione proprietaria della banca dati centralizzata.

Come detto, questa nuova forma di pubblicità agevola l'attività delle amministrazioni che, a seguito della riforma, non sono più tenute a comunicare le medesime informazioni alle banche dati centralizzate e, contestualmente, a pubblicarle sul sito della trasparenza del proprio ente replicando più volte la medesima attività. Diversamente, sarebbe condizionata negativamente l'efficienza dell'attività amministrativa e si correrebbe il rischio di incappare nell'errore pubblicando dati difformi rispetto a quelli comunicati ad organi centrali.

Una disposizione volta a “favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e prevenire fenomeni di corruzione, si utilizza la «Banca dati nazionale dei contratti pubblici» (BDNCP) gestita dall'Autorità Nazionale Anticorruzione ai sensi dell'articolo 213 del decreto legislativo 18 aprile 2016, n. 50” trova anche trattazione nel C.A.D. art. 62-bis rubricato “Banca dati nazionale dei contratti pubblici”. Al di là del riferimento contenuto nel citato art. 62-bis del C.A.D. alla BDNCP, tutte le banche dati per le quali è prevista la possibilità della pubblicazione sostitutiva sono elencate puntualmente e tassativamente nell’allegato B al d.lgs. 33/2013.

Nome della banca dati	Amm. che detiene la banca dati	Norma/e istitutiva/e della banca dati	Obblighi previsti dal d.lgs. n. 33 del 2013
Perla PA	PCMDFP	- Artt. 36, co. 3, e 53 del d.lgs. n. 165 del 2001; - art. 1, co. 39-40, della legge n. 190 del 2012	Art. 15 (titolari di incarichi di collaborazione o consulenza); art. 17 (dati relativi al personale non a tempo indeterminato); art. 18 (dati relativi agli incarichi conferiti ai dipendenti pubblici)
SICO – Sistema Conoscitivo del personale dipendente dalle Amministrazioni pubbliche	MEFRGS (IGOP)	Artt. 40-bis, co. 3, e 58-62 del d.lgs. n. 165 del 2001	Art. 16, co. 1-2 (dotazione organica e costo del personale con rapporto di lavoro a tempo indeterminato); art. 17 (dati relativi al personale non a tempo indeterminato); art. 21, co. 1 (dati sulla contrattazione collettiva nazionale); art. 21, co. 2 (dati sulla contrattazione integrativa)
Archivio contratti del settore pubblico	ARAN CNEL	Artt. 40-bis, co. 5, e 47, co. 8, del d.lgs. n. 165 del 2001	Art. 21, co. 1 (dati sulla contrattazione collettiva nazionale); art. 21, co. 2 (dati sulla contrattazione integrativa)
SIQuEL – Sistema Informativo Questionari Enti Locali	Corte dei conti	Art. 1, co. 166-167, della legge n. 266 del 2005	Art. 22 (dati relativi ai soli Enti locali riguardanti enti pubblici vigilati, enti di diritto privato in controllo pubblico, partecipazioni in società di diritto privato)
Patrimonio della PA	MEF-DT	- Art. 2, co. 222, della legge n. 191 del 2009; - art. 17, co. 3-4, del decreto legge n. 90 del 2014, convertito, con modificazioni, dalla legge n. 114 del 2014	Art. 22, commi 1 e 2 (dati relativi a società, enti pubblici e enti di diritto privato partecipati dalle amministrazioni pubbliche o in cui le Amministrazioni nominano propri rappresentanti negli organi di governo); art. 30 (dati relativi a beni immobili posseduti o detenuti delle amministrazioni pubbliche)
Rendiconti dei gruppi consiliari regionali	Corte dei conti	- Art. 1, co. 10, del decreto legge n. 174 del 2012, convertito, con modificazioni, dalla legge n.	Art. 28, co. 1 (pubblicità dei rendiconti dei gruppi consiliari regionali)

		213 del 2012; - d.P.C.M. 21 dicembre 2012	
BDAP – Banca Dati Amministrazioni Pubbliche	MEFRGS	- Art. 13 della legge n. 196 del 2009; - decreto del Ministro dell'economia e delle finanze n. 23411 del 2010; - d.lgs. n. 229 del 2011; - d.lgs. n. 228 del 2011;	Art. 29, co. 1 (bilanci preventivi e consuntivi delle amministrazioni pubbliche) Art. 37, comma 1, lett. a), b), c) (informazioni relative alle procedure per l'affidamento e l'esecuzione di opere e lavori) Art. 38, Pubblicità dei processi di pianificazione, realizzazione e valutazione delle opere pubbliche
REMS (Real Estate Management System) – Sistema di Gestione degli Immobili di Proprietà Statale	Demanio		Art. 30 (beni immobili e gestione del patrimonio)
BDNCP – Banca Dati Nazionale Contratti Pubblici	ANAC	- Art. 62-bis del d.lgs. n. 82 del 2005; - art. 6-bis del d.lgs. n. 163 del 2006	Art. 37, co. 1 (informazioni relative alle procedure per l'affidamento e l'esecuzione di opere e lavori pubblici, servizi e forniture)
Servizio Contratti Pubblici	MIT	Artt. 66, co. 7, 122, co. 5 e 128, co. 11, del d.lgs. n. 163 del 2006	Art. 37, co. 1 (informazioni relative alle procedure per l'affidamento e l'esecuzione di opere e lavori pubblici, servizi e forniture)

La previsione di questa nuova modalità di pubblicazione ha, tuttavia delle conseguenze per il cittadino. Infatti, può accadere che il cittadino non riesca ad ottenere le informazioni oggetto di pubblicazione obbligatoria dalla banca dati centralizzata a cui accede tramite il link pubblicato nell'apposito spazio "Amministrazione trasparente" dell'amministrazione che conferisce il dato. In tal caso avrà difficoltà ad individuare a chi rivolgere la propria richiesta di accesso civico semplice. Sarà difficile per lui capire se vi sia stato un difetto di comunicazione dall'amministrazione conferente l'informazione alla banca dati o se l'inadempienza sia da attribuire a quest'ultima. E la difficoltà ad individuare l'inadempiente comporterà, conseguentemente, anche quella di individuare il soggetto azionabile in quanto dotato del potere sostitutivo.

6.6 Accesso e privacy

Il tema del bilanciamento tra l'interesse a conoscere e quello alla riservatezza, già affrontato problematicamente dalla giurisprudenza fin dall'applicazione delle norme sull'accesso documentale ex l. 241/920, ha trovato una elaborazione composita all'indomani dell'introduzione nel nostro ordinamento degli istituti di accesso semplice e generalizzato. Con l'istituzione delle norme sull'accesso di cui al d.lgs. 97/2016 il rapporto tra privacy e trasparenza si arricchisce di un ulteriore

elemento di complessità. Tale rapporto, infatti, finisce con il richiedere una coniugazione differente asseconda che si tratti di diritto di accesso documentale classico, semplice o generalizzato.

L'art. 2, comma 1 del d.lgs. 33/2013 riformato recita: "Le disposizioni del presente decreto disciplinano la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione". Il legislatore pone qui il problema del contemperamento tra il diritto di accesso ai dati, così come ampliato dal d.lgs. 97/2016, ed i limiti posti allo stesso dai rilevanti interessi pubblici (sicurezza pubblica e ordine pubblico, sicurezza nazionale, difesa e questioni militari, relazioni internazionali, politica e stabilità finanziaria ed economica dello Stato, conduzione di indagini sui reati e il loro perseguimento, regolare svolgimento di attività ispettive) e privati (protezione dei dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali); tuttavia, non delimita questi due ambiti ma si limita ad enunciare il principio generico della necessità del contemperamento del diritto di accesso e del diritto di opposizione all'accesso.

Già all'indomani dell'emanazione del d.lgs. 33/2013, il Garante per la protezione dei dati personali era intervenuto ritendendo di dover "individuare un quadro organico e unitario di garanzie finalizzato a indicare apposite cautele in relazione alle ipotesi di diffusione di dati personali mediante la pubblicazione sui siti web da parte di organismi pubblici e in particolare di quelli chiamati a dare attuazione al d.lgs. n. 33/2013 attraverso l'adozione di nuove "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"". In ragione di ciò, sono state pubblicate sulla **Gazzetta Ufficiale n. 134 del 12 giugno 2014 apposite Linee guida (doc. web n. 3134436)**. Uno dei principi che secondo il Garante dovrebbe ispirare l'azione delle amministrazioni è che, in tutti i casi, "indipendentemente dalla finalità perseguita, laddove la pubblicazione online di dati, informazioni e documenti, comporti un trattamento di dati personali, dovranno essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

Con la riforma del 2016, il legislatore ha cercato di indicare regole più certe utili per addivenire ad un giusto bilanciamento tra trasparenza e privacy. A questa finalità risponde il nuovo art. 7-bis del decreto trasparenza.

Secondo il legislatore, tutti i dati oggetto di pubblicazione obbligatoria devono essere pubblicati senza che a questi possa essere opposto alcun diritto alla riservatezza poiché la trasparenza pubblica "integra una finalità di rilevante interesse pubblico". Sicché, i dati oggetto di pubblicazione obbligatoria che non siano dati sensibili, sensibilissimi o giudiziari, possono essere diffusi attraverso i siti istituzionali, sottoposti ad indicizzazione tale da consentire il loro rinvenimento tramite motori di ricerca e fatti oggetto di riuso. L'unico limite è costituito dal rispetto dei principi sul trattamento dei dati personali (non eccedenza, proporzionalità, pertinenza, correttezza, esattezza). I soggetti tenuti alla pubblicazione obbligatoria devono obliare i dati sensibili o giudiziari che non siano essenziali a soddisfare quella finalità di trasparenza specifica ovvero i dati non pertinenti la cui pubblicazione valicherebbe i confini dell'utilità pubblica che la trasparenza si prefigge.

Nell'ipotesi dell'istituto dell'accesso generalizzato, i limiti di cui all'art. 5-bis consentono di sottrarre all'accesso i dati la cui conoscenza pregiudicherebbe "concretamente" interessi pubblici e privati elencati nel medesimo articolo citato. Lì dove l'amministrazione è in condizione di anonimizzare in modo efficace i documenti contenenti tali dati, tanto da garantire sia l'interesse all'informazione che quello alla protezione dei dati, il diritto di accesso è riconosciuto. Lì dove tale anonimizzazione non è realizzabile in modo efficace, l'amministrazione deve valutare la concretezza del pregiudizio derivabile alla riservatezza dal consenso all'esercizio dell'accesso. Il legislatore, consapevole della difficoltà di porre in equilibrio l'interesse della trasparenza e quello della privacy, ha affidato all'ANAC il compito di definire in apposite Linee guida, adottate d'intesa con il Garante per la protezione dei dati personali, le "indicazioni operative" utili alle amministrazioni.

Appare opportuno richiamare qui gli effetti delle modifiche apportate dalla novella di cui al d.lgs. 97/2016 all'art. 14 del d.lgs. 33/2013 che hanno comportato una estensione notevole dell'ambito soggettivo di applicazione degli obblighi di pubblicazione di cui al comma 1 del citato articolo anche ai dirigenti. Nel codice trasparenza previgente alla riforma del 2016, infatti, l'art. 15 distingueva gli obblighi di comunicazioni a carico dei dirigenti - che restavano quelli di cui all'art. 17, comma 22 della legge 15 maggio 1997, n. 127 - dagli obblighi di pubblicazione che riguardavano gli estremi dell'atto di conferimento dell'incarico; il curriculum vitae; i dati relativi allo svolgimento di incarichi o la titolarità di cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione o lo svolgimento di attività professionali; i compensi, comunque

denominati, relativi al rapporto di consulenza o di collaborazione, con specifica evidenza delle eventuali componenti variabili o legate alla valutazione del risultato.

Con la riforma del 2016, gli obblighi di trasparenza in capo ai dirigenti sono disciplinati non più dall'art. 15 ma dal novellato art. 14 che al nuovo comma 1-bis assimila la posizione dei titolari di incarichi dirigenziali a quella dei titolari di incarichi politici facendo coincidere gli obblighi di pubblicazione degli uni a quelli degli altri. In conseguenza di ciò, i dirigenti nonché il coniuge non separato ed i parenti entro il secondo grado sono tenuti alla pubblicazione, e non soltanto alla comunicazione come era in precedenza, di tutte le dichiarazioni di cui agli artt. 2, 3 e 4 della legge 5 luglio n. 441. In questa nuova formulazione della norma qualcuno ha osservato (OLIVERI) che l'assimilazione della posizione di chi ricopre incarichi politici a quella dei dirigenti è errata nei suoi presupposti. Il dirigente entra a far parte dei ruoli dell'amministrazione con contratti individuali di diritto privato a seguito di selezione concorsuale ed è soggetto a valutazione del raggiungimento di propri obiettivi ai sensi dell'art. 21 del d.lgs. 165/2001. Di tutt'altra natura la posizione di chi ricopra incarichi elettivi politici.

Lo stesso Garante, rilasciando il 3 marzo 2016 il proprio parere sullo schema di decreto legislativo concernente la revisione e semplificazione delle disposizioni di prevenzione della corruzione, pubblicità e trasparenza, si è espresso in termini critici sul contenuto del nuovo art. 14 che ha radicalmente modificato il quadro degli obblighi previgenti ed ha richiamato l'attenzione della presidenza del Consiglio dei Ministri su "l'importanza di un approccio rispettoso del principio di proporzionalità di derivazione europea (art. 6, par. 1, lett. c, dir. 95/46/CE), che tenga in considerazione l'orientamento espresso dalla Corte di giustizia nelle sentenze del 20 maggio 2003 (Cause riunite C-465/00, C-138/01 E C-139/01, Rechnungshof e al.), del 9 novembre 2010 (Cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e al.) e del 29 giugno 2010 (Causa C-28/08P, Commissione/Bavarian Lager). Secondo tale orientamento, le istituzioni pubbliche, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l'interesse dell'Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE, senza che possa riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali, anche qualora siano coinvolti rilevanti interessi economici (par. 85, sentenza Volker und Markus Schecke GbR e al.)". Il Governo, tuttavia, non si è uniformato alle osservazioni del Garante.

In fase, quindi, di applicazione della norma, avverso l'art. 14, comma 1-bis nella parte in cui prevede che le amministrazioni pubblichino i dati di cui all'art. 14, comma 1 lettere c) ed f), sono stati proposti ricorsi al TAR da parte di alcuni dirigenti pubblici e di dirigenti di autorità indipendenti tra i quali anche alcuni in servizio presso il Garante privacy. I ricorrenti ritengono,

infatti, che nella disposizione impugnata vi siano dei profili di incostituzionalità e incompatibilità con le norme di diritto comunitario. Il giudice amministrativo ha considerato la questione materia di trasparenza amministrativa e rifacendosi ai contenuti dell'art. 50 del d.lgs. 33/2013 ha affermato la propria giurisdizione esclusiva. Quindi, si è espresso ritenendo significativi i rilievi sollevati nel ricorso e valutando "l'irreparabilità del danno paventato dai ricorrenti discendente dalla pubblicazione on line, anche temporanea, dei dati per cui è causa", ha dapprima sospeso con ordinanza cautelare (**TAR Lazio, sez. I-quater, ordinanza n. 1030/2017**), ha deciso la sospensione dell'efficacia delle note con le quali le amministrazioni di appartenenza richiedevano ai dirigenti ricorrenti, ai fini della pubblicazione nel sito web, i dati di carattere reddituale e patrimoniale previsti dall'art. 14, comma 1, lett. c) ed f) del d.lgs. 33/2013. Nell'immediatezza della sentenza, ANAC è intervenuta con una propria azione di indirizzo deliberando di "sospendere l'efficacia della delibera n. 241/2017 "Linee guida recanti indicazioni sull'attuazione dell'art. 14 del d. lgs. 33/2013 «Obblighi di pubblicazione concernenti i titolari di incarichi politici, di amministrazione, di direzione o di governo e i titolari di incarichi dirigenziali» come modificato dall'art. 13 del d.lgs. 97/2016", limitatamente alle indicazioni relative all'applicazione dell'art. 14 co. 1, lett. c) ed f) del d. lgs. n. 33/2013 per tutti i dirigenti pubblici, compresi quelli del SSN, in attesa della definizione nel merito del giudizio o in attesa di un intervento legislativo chiarificatore (**ANAC, Delibera n. 382 del 12 aprile 2017**).

Il **TAR Lazio (Roma), sez. I-quater, ordinanza n. 9828** rimette alla corte costituzionale la decisione sulla legittima costituzionale della pubblicazione dei dati di cui all'art. 14, comma 1, lett. c) ed f) del decreto trasparenza poiché il giudice ha ritenuto non manifestamente infondata e rilevante la questione sottopostagli ed ha rimesso la decisione al giudice costituzionale ritenendo la norma in parte qua in contrasto con i principi di ragionevolezza e di uguaglianza di cui all'art. 3 Cost. nonché con i principi in tema di tutela della privacy ex art.117 Cost. Il giudice sostiene che l'obbligo di trasparenza, imposto dall'articolo 14 del suddetto d.lgs. n. 33/2013, con l'intento di evitare fenomeni di corruzione amministrativa, nel bilanciamento tra privacy e trasparenza, non va a contemperare equamente le esigenze di tutela dei dirigenti, sacrificando irragionevolmente il diritto di questi a non rendere note a terzi i dati personali pubblicati sui siti istituzionali dell'amministrazione. Il giudice adito ha ritenuto di rimettere la decisione al giudice costituzionale in quanto "la tutela della posizione dei ricorrenti, che consegue alla rilevata serietà delle contestazioni formulate,[…] , non può essere attuata mediante l'annullamento degli atti gravati, trattandosi, […] di provvedimenti che danno mera esecuzione a puntuali obblighi di legge". Inoltre, il giudice ritiene che la norma contestata dai ricorrenti non sia suscettibile di essere disapplicata per contrasto con normative comunitarie, ciò in considerazione del fatto che, non è individuabile una

disciplina self-executing di tale matrice direttamente applicabile alla fattispecie oggetto di giudizio. Alla Corte Costituzionale spetta decidere se la norma di cui si tratta sia o meno in contrasto con gli artt. 117, comma 1, 3, 2 e 13 della Costituzione.

CAPITOLO 7
OPEN GOVERNMENT E OPEN DATA

1. Introduzione: del rapporto tra trasparenza, tecnologia e diritti

Le tecnologie ICT (*Information and Communication Technologies*) hanno avuto un impatto pervasivo sulla società contemporanea sia nella dimensione collettiva, che in quella individuale. Con l'emanazione del Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) il legislatore ha perseguito lo scopo di rendere la P.A. digitale e capace di relazionarsi efficientemente con i cittadini e con le imprese per mezzo dei nuovi strumenti tecnologici. In tale processo un ruolo chiave spetta alla trasparenza, senza la quale l'altro elemento centrale, ovvero l'informazione, risulterebbe incompleto e limitato. La trasparenza, infatti, è in grado di garantire il buon andamento e l'imparzialità dell'azione dell'amministrazione in quanto permette il controllo democratico, contribuendo così ad orientare correttamente l'azione dei pubblici poteri in direzione delle reali necessità dei cittadini (FAINI). La nozione di trasparenza/pubblicità in questo ambito è incentrata sulla progressiva individuazione di ulteriori "elementi conoscitivi" che la pubblica amministrazione deve rendere disponibili *online* sul proprio sito istituzionale, col preciso scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità (CARLONI). La trasparenza, dunque, trova un alleato nell'informatizzazione, dal momento che le tecnologie ICT – in particolare internet ed il web – sono capaci, per il loro carattere ubiquitario, di rendere le informazioni disponibili ad un numero indefinito di soggetti ed agevolare la partecipazione dei cittadini alle politiche intraprese dal Governo (locale o nazionale) e di pronunciarsi su queste con strumenti informali.

La **trasparenza** si è evoluta nella duplice prospettiva della **piena accessibilità delle informazioni**, ma anche di una **amministrazione come organizzazione aperta e al servizio dei cittadini**, che deve operare con efficacia ed efficienza, garantendo così la buona qualità della sua azione. In questa nuova dimensione l'accessibilità delle informazioni diventa uno strumento partecipativo che contribuisce a costruire un corretto rapporto tra amministrazione e cittadino ed a rendere le scelte maggiormente condivise. Nella medesima ottica il Codice della Trasparenza (d.lgs. n. 33/2013) pone la base su cui costruire una nuova concezione di amministrazione aperta, secondo un percorso

già intrapreso da qualche anno. Una premessa indispensabile per il **buon funzionamento della società democratica** consiste nel **garantire ed ampliare l'area della partecipazione attiva e consapevole alle scelte politiche e amministrative**, unita al controllo sulle medesime. Infatti, gli studi riportano riscontri della relazione positiva tra un pubblico di cittadini informati e la qualità del tessuto sociale della propria comunità, la fiducia nelle istituzioni e servizi più efficienti; vi sarebbe dunque un legame positivo tra alti livelli di partecipazione al processo decisionale e la migliore qualità dei prodotti e dei servizi (SARTORI). La trasparenza amministrativa, intesa come la messa a disposizione del patrimonio informativo pubblico, costituisce quindi la base per una nuova relazione amministrazione-cittadini, impegnati entrambi nella miglior cura dell'interesse pubblico.

In un'**economia basata sulla conoscenza**, dove la quantità e la qualità dell'informazione rappresentano un valore enorme, **un luogo di raccolta dati aperti, aggiornati e certificati, come sono le piattaforme che realizzano politiche di *open government*, deve essere ritenuta una infrastruttura** al pari di un'autostrada o un aeroporto. Il modello dell'*open government* e dell'*open data* sta vivendo una grande diffusione in un momento storico in cui sono necessari strumenti utili a razionalizzare la spesa ed a migliorare la gestione della cosa pubblica, allo scopo di garantire maggiormente i diritti delle persone. Le più recenti modifiche al Codice dell'Amministrazione Digitale (CAD) e gli interventi in materia di trasparenza ed accesso civico pongono l'accento proprio sulla necessità di provvedere alla riorganizzazione ed aggiornamento dei servizi resi, posto che attraverso l'uso delle tecnologie informatiche è possibile valutare le esigenze dei cittadini e renderli partecipi delle scelte pubbliche. Le ICT, infatti, consentono di migliorare i servizi, adeguandoli alle aspettative dei cittadini dal punto di vista del contenimento dei tempi necessari all'erogazione e dei costi. Dall'altro lato l'uso delle tecnologie informatiche permette di contenere le disuguaglianze fisiche e sociali che impediscono un uguale accesso alle informazioni ed ai servizi. Tuttavia, per il pieno raggiungimento dello scopo occorrerebbe avviare un percorso generalizzato di alfabetizzazione che permetta a tutti i cittadini di fruire degli strumenti informatici, superando un eventuale *digital divide.*

A livello legislativo i **principi dell'*open government*** si basano su tre grandi **architravi**. La prima è data dalla **normativa comunitaria in materia di riutilizzo dei documenti delle informazioni del settore pubblico** (PSI) (Direttiva 2013/37/UE del 26.06.2013, che ha modificato la Direttiva 2003/98/CE). La seconda è data dal **Codice dell'Amministrazione digitale**; la terza è data dal **Codice della trasparenza**, che detta regole volte espressamente a favorire l'affermazione di un modello di amministrazione aperta.

1. Le politiche sovrannazionali per la crescita digitale

L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) è stata tra i primi ad impegnarsi nel promuovere il processo di *e-government* pensando alle tecnologie informatiche come strumenti utili allo scopo di combattere la corruzione e avvicinare le P.A. ai bisogni dei cittadini, in modo da rafforzare la loro fiducia nelle istituzioni pubbliche.

L'***e-government*** può essere definito come il **processo che, attraverso l'utilizzo delle tecnologie ICT, mira a trasformare le relazioni interne ed esterne alla P.A. ed a migliorare l'erogazione dei servizi, attraverso l'incremento della partecipazione dei vari attori pubblici, migliorando così la qualità di amministrazione dei soggetti pubblici**.

L'OCSE, nello studio "*Citizens As Parteners. Information, Consultation and Public Participation in Policy Making*" del 2001 sottolineava la necessità di ampliare il coinvolgimento dei cittadini, tenendo conto delle loro opinioni nei processi decisionali, al fine di migliorare la qualità delle politiche pubbliche e di rispondere alla crescente domanda di trasparenza dell'operato degli attori pubblici e, infine, di rafforzare la fiducia dei cittadini verso le istituzioni per contrastare il declino della partecipazione elettorale attiva. L'OCSE ha così individuato tre livelli principali di coinvolgimento: informazione, consultazione e partecipazione attiva. Inoltre, la democrazia elettronica era indicata come risposta alla necessità delle P.A. di far fronte alla crescente complessità delle decisioni, mediante un coinvolgimento più ampio delle competenze e delle esperienze diffuse nella società (RABBITO).

Inoltre, nel 2008 l'OCSE ha emanato la raccomandazione "*For Enhanced Access and More Effective Use of Public Sector Information"*, che aveva come intento quello di promuovere la diffusione dei dati pubblici, dettando condizioni trasparenti per il riuso, ovvero gratuità, trasparenza, rispetto del diritto di autore, oltre alla possibilità di fare ricorso a *partnership* pubblico-private per rendere disponibili le informazioni. Nel documento l'OCSE considerava "*the use of ITCs, and particulary the Internet, as a tool to achieve better government"*. Tra gli scopi principali dell'*e-government*, quindi, vi è quello di avvicinare i poteri pubblici ai soggetti amministrati in modo da favorire il passaggio da un modello organizzativo centralizzato ed autoritario, ad uno consensuale e partecipativo, che renda i destinatari dei servizi utenti di amministrazioni efficienti, efficaci e trasparenti.

A livello comunitario, le radici dell'idea dell'*open government* possono rintracciarsi nel Trattato sul Funzionamento dell'Unione Europea (TFUE), dove tra i principi relativi alla P.A. troviamo la richiesta che essa sia "aperta, efficace, trasparente" (art. 298). La Strategia di Lisbona, basandosi su queste tre caratteristiche, ha riconosciuto un ruolo fondamentale alla diffusione delle tecnologie informatiche per costruire un'amministrazione ed un'economia efficienti, dinamiche e trasparenti. In base a tale strategia l'obiettivo primario deve essere quello di far diventare l'Unione uno spazio

di competenze basato sulla conoscenza, per essere competitiva e dinamica rispetto agli altri paesi anche attraverso la creazione di un'economia basata sull'innovazione.

La direttiva 2003/98/CE (recepita dall'ordinamento italiano con il d.lgs. n. 36/2006) ha attribuito a ciascuna P.A. la possibilità di permettere il riutilizzo delle informazioni che ognuna di esse raccoglie, produce o diffonde nell'ambito del perseguimento dei propri compiti istituzionali. Alla base della Direttiva sta la considerazione per cui i dati detenuti dai soggetti pubblici costituiscono una risorsa da sfruttare per la crescita economica e per la creazione di posti di lavoro. In particolare, per "riutilizzo" la Direttiva intende "l'uso di documenti in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali, diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i documenti sono stati prodotti. Lo scambio di documenti tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico non costituisce riutilizzo". La direttiva parte dal presupposto in base al quale rendere pubbliche le PSI (*Public Sector Information*) rappresenta uno strumento fondamentale per ampliare il diritto alla conoscenza, principio cardine della democrazia ed obiettivo applicabile alle istituzioni ad ogni livello. Alla direttiva 2003/98/CE è succeduta la direttiva 2007/2/CE del 14.03.2007, denominata INSPIRE, la quale puntava a creare un'infrastruttura per l'informazione territoriale nell'Unione.

Nel dicembre 2011, la Commissione ha poi presentato una strategia relativa al tema degli *open data*, che include la Comunicazione della Commissione Europea *"Dati aperti: un motore per l'innovazione, la crescita e una governance trasparente"* del 12.12.2011, una proposta di modifica della Direttiva del 2003 ed una Decisione della Commissione relativa al riutilizzo delle informazioni in possesso della Commissione stessa (2011/833/UE). In seguito alla proposta di modifica della direttiva il 26.06.2013, il Parlamento Europeo e il Consiglio hanno approvato la direttiva 2013/37/UE, che reca una modifica della regolazione del riutilizzo dell'informazione del settore pubblico la quale, per la prima volta, estende in particolare la sua applicazione al settore culturale (archivi, musei, biblioteche) allo scopo di favorire l'armonizzazione delle legislazioni dei singoli Stati membri.

Tali finalità, di ordine generale, devono essere incluse nel contesto della politica sovrannazionale definita con l'Agenda Digitale Europea (Comunicazione Commissione COM(2010)245 del 26.08.2010), a sua volta individuata come una delle iniziative-faro del programma "Europa 2020: una strategia per la crescita intelligente, sostenibile e inclusiva" (COM(2010)2020, del 03.04.2010). La strategia Europa 2020 mira a promuovere una crescita intelligente, sostenibile e solidale, basando il raggiungimento degli obiettivi anche sull'innovazione. Infatti, l'Agenda Digitale Europea propone di sfruttare al meglio il potenziale delle tecnologie dell'informazione e della comunicazione per favorire innovazione, crescita economica e progresso. L'Agenda digitale Europea ha come

obiettivo primario quello di promuovere la crescita economica e dell'occupazione investendo sulla diffusione delle ICT, sulla creazione di nuove infrastrutture per i servizi pubblici digitali, sulla realizzazione di una nuova strategia industriale dell'elettronica e sul *cloud computing*. Il *cloud comuputing* è un sistema che consente di erogare servizi a richiesta attraverso la rete – come risorse di archiviazione, software e database – nel quale il pagamento dei servizi avviene secondo l'utilizzo, evitando i costi di investimento. I dati vengono archiviati o elaborati da terminali virtuali ubicati su server non appartenenti all'amministrazione (COSTANTINO). L'utilizzo del modello *cloud computing* risulta particolarmente significativo per la pubblica amministrazione in quanto esso comporta vantaggi strategici legati alla possibilità di conseguire sia l'ammodernamento delle infrastrutture, sia la condivisione di sistemi, applicazioni e banche dati, con l'obiettivo finale di realizzare servizi pubblici efficaci e di qualità. La Comunicazione della Commissione COM (2012)529 del 27.09.2012 detta indirizzi mirati a favorire l'utilizzo del *cloud computing* all'interno dell'Unione. L'Agenzia per l'Italia digitale ha emanato due circolari sul tema, entrambe pubblicate in G.U. n. 92/2018. La circolare n. 2 del 09.04.2018 che stabilisce i criteri per la qualificazione dei Cloud Service Provider per la P.A.; la circolare n. 3 del 09.04.2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della P.A.

In questo quadro risulta centrale lo sviluppo di politiche di *e-government* come motore di sviluppo economico e come strumento di promozione di una democrazia maggiormente partecipata dai cittadini. Infatti, secondo la Commissione, i servizi di *e-government* costituiscono un modo per migliorare il servizio ai cittadini e alle imprese, favorire la partecipazione e promuovere un'amministrazione aperta e trasparente. La Commissione Europea si propone di realizzare tali priorità attraverso la costruzione di un *Digital Single Market* basato su internet ad alta velocità e su applicazioni interoperabili, attraverso l'investimento nella ricerca e nell'innovazione, favorendo l'alfabetizzazione e il miglioramento delle competenze digitali, le quali vengono incluse tra le priorità del Fondo Sociale Europeo. Tra gli obiettivi del *Digital Single Market* vi è anche la promozione dell'*open government*.

Quella dell'Agenda Digitale è una politica che parte dal livello comunitario per poi svilupparsi a livello nazionale e locale; in questo contesto si collocano anche le strategie per la digitalizzazione delle pubbliche amministrazioni, sia comunitarie che nazionali, che sono volte al miglioramento dei servizi delle amministrazioni e della vita quotidiana dei cittadini, allo sviluppo della competitività ed alla crescita economica. Dal momento che la maggior parte del PIL dell'Unione finanzia la spesa pubblica, la disciplina delle modalità attraverso cui le amministrazioni erogano i servizi, scelgono i contraenti, decidono di finanziare una certa opera o un certo servizio, sono decisive per la determinazione del modello di democrazia – non solo di amministrazione – che viene promosso a

livello comunitario. Per realizzare gli obiettivi posti dalla legislazione comunitaria, dunque, l'Agenda Digitale Italiana (prevista dall'art. 47 del d.l. 5/2012, convertito nella l. 35/2012) ha favorito modelli di *open government* volti ad incrementare la collaborazione tra le amministrazioni, la trasparenza dell'azione pubblica e la partecipazione dei privati ai procedimenti amministrativi.

2. Il rapporto tra le politiche di *openess* e il principio del buon andamento

Le politiche di *openess* possono essere indirettamente ricondotte all'art. 97 della Costituzione. Infatti, uno dei pilastri della prassi amministrativa dell'*open government* è individuato nella **trasparenza, in quanto strumento di attuazione dei principi di imparzialità e buon andamento** che devono governare l'attività amministrativa. Il processo che dalla liberazione del dato pubblico porta alla creazione di nuova trasparenza trova non solo legittimazione ma anche incoraggiamento nella Costituzione, in quanto favorisce la piena attuazione dei principi di eguaglianza, imparzialità, buon andamento e sussidiarietà orizzontale (MANCOSU). L'*open data* potrebbe essere letto come una precondizione dell'effettività dei principi e dei diritti fondamentali sanciti dalla Costituzione, in quanto se il dovere di trasparenza impone all'amministrazione la visibilità dei suoi percorsi decisionali, esso prescrive anche l'esibizione dei risultati del suo agire pubblico, cioè i dati.

L'organizzazione dei pubblici uffici e l'attività amministrativa in generale, essendo orientata allo sviluppo della persona, alla crescita economica, al benessere fisico e sociale dei cittadini deve rispondere all'esigenza per la quale è stata programmata, adattandosi ai mutamenti derivanti dall'evolversi della società. Dal momento che il buon andamento è ritenuto anche un principio di organizzazione, nel senso che esso rappresenta l'idoneità dell'organizzazione a perseguire l'obiettivo (Corte Costituzionale, sentenza n. 123/1968; NIGRO) allora la tecnologia informatica, migliorando l'organizzazione, con conseguente miglioramento dei processi contribuisce per ciò solo all'attuazione del principio del buon andamento. Consegue da quanto detto che le politiche di *open government*, sfruttando lo sviluppo di tecnologie che agevolano l'uso del digitale nei rapporti interni tra pubbliche amministrazioni e nei rapporti esterni, tra amministrazione e cittadini, incentivano nuove forme di collaborazione e per questo contribuiscono all'attuazione del principio del buon andamento.

2. Le politiche di *open government*

2.1. Dal *New Public Management* alla *Digital Era Governance*

La teorizzazione dell'*open government* è avvenuta grazie alla possibilità da parte di soggetti pubblici di utilizzare le tecnologie. Negli anni '90 il modello di amministrazione, indicato come

New Public Management (NPM), era basato sull'*outsourcing*, ossia sull'idea di utilizzare il settore privato in luogo di quello pubblico. Per la gestione della cosa pubblica il modello NPM si ispirava a criteri aziendalistici basati sul risultato, in cui il cittadino era visto come utente o consumatore. Elemento caratterizzante era l'individuazione di indicatori di prestazione (*performance indicators*) sulla base dei quali misurare o valutare i prodotti, i livelli di servizio ed i risultati conseguiti (OSBORNE, GAEBLER). Tale modello, in altri termini, adottava logiche e strumenti delle aziende private, che venivano ritenuti in grado di soddisfare i cittadini – intesi come utenti o consumatori – in modo efficace, migliorando i servizi e facilitando l'accesso ad essi.

A partire dal nuovo millennio ha iniziato a diffondersi un nuovo approccio alla gestione pubblica – non opposto al NPM – indicato con il nome di *Digital Era Governance* (o anche *Public Governance*). La riflessione circa gli assetti istituzionali che regolano i rapporti tra i poteri pubblici ed i cittadini ha preso le mosse dalla considerazione secondo cui la missione delle istituzioni pubbliche non si esaurisce nell'assicurare servizi pubblici efficienti, ma richiede un legame tra le organizzazioni pubbliche e le comunità di riferimento che migliori la fiducia nelle istituzioni e che sia espressione di uno Stato democratico e trasparente.

La ***Digital Era Governance*** (DEG) implica una **nuova concezione del ruolo della P.A.** nei confronti degli altri attori sociali (imprese, cittadini, associazioni) **orientata al raggiungimento degli obiettivi privilegiando l'utilizzo degli strumenti del consenso e dell'economicità**. In base a tale concezione, per fronteggiare la complessità nell'individuare *policies* adeguate le P.A. devono strutturare sistemi di *governance* collaborativa nella gestione della cosa pubblica. In quest'ottica, la collaborazione ha lo scopo di migliorare la gestione e raggiungere efficacemente gli obiettivi prefissati. Nel modello DEG il cittadino è visto come un collaboratore (DUNEAVY), come risorsa, il che può essere letto come una declinazione del principio di sussidiarietà orizzontale.

Alla base del modello vi sono tre **elementi chiave: riportare la gestione sotto il controllo pubblico, riorganizzare la gestione amministrativa interna in riferimento a distinti gruppi** (*stakeholders*) e **la digitalizzazione**, intesa come il pieno sfruttamento del potenziale del *digital storage* e della comunicazione via internet, allo scopo di trasformare l'organizzazione delle P.A. In altri termini, contrariamente al *New Public Management*, che sollecitava una diminuzione dell'intervento pubblico in favore di quello privato, nel nuovo paradigma risulta centrale la creazione di un rapporto trasparente tra P.A. e cittadini. In tale modello un ruolo essenziale rivestono i paradigmi di *e-government* e, nella successiva evoluzione, dell'*open government*, i quali offrono strumenti utili al raggiungimento degli obiettivi posti dalla dottrina DEG.

L'*e-government* ha creato un modello integrato di gestione delle informazioni basato sulla condivisione di esse dalle diverse P.A., dal momento che l'ottimizzazione del *data storage*

attraverso la dematerializzazione delle informazioni comporta lo snellimento delle procedure burocratiche, la razionalizzazione della gestione del patrimonio informativo pubblico e, in ultima istanza, la riduzione dei costi di gestione. In definitiva, il processo di ammodernamento caratterizzato dall'implementazione dell'uso delle tecnologie ICT nel sistema pubblico ha costretto le amministrazioni ad iniziare un processo di trasformazione, che coinvolge sia la collaborazione tra soggetti pubblici, sia attività erogative di servizi verso i cittadini.

2.2. I fondamenti del modello dell'amministrazione aperta

A livello nazionale, le esigenze di apertura (*openess)* possono essere ricondotte ad un concetto avanzato di trasparenza, da intendere come condizione complessiva di conoscibilità ed *accountability*, a vantaggio della generalità dei cittadini. In questo senso tale dottrina, che presuppone forme di conoscenza generalizzate, si contrappone ad istituti come il diritto di accesso, che ha un campo di applicazione più circoscritto (CARLONI). La novità della dottrina, tuttavia, non è limitata al regime di accessibilità totale, ma fa anche riferimento a dinamiche di comunicazione ed interazione bidirezionale tra il cittadino e la P.A., cioè a forme di interazione basate sulla condivisione e sulla partecipazione ai processi decisionali pubblici, rese possibili dallo sviluppo tecnologico.

Quello dell'*open government* può essere considerato come un percorso innovativo che coinvolge la dimensione organizzativa, gestionale, relazionale, informativa e culturale del sistema pubblico. **L'*open government* ridefinisce il rapporto tra P.A. e cittadini, spostando il focus da un approccio orientato ad erogare un servizio, ad uno basato sul processo di collaborazione tra amministrazione e cittadini**. L'apertura della P.A. dovrebbe contribuire a **costruire una relazione con il cittadino basata sulla fiducia**. L'*open government*, di conseguenza, può essere definito come un modo di essere e di dover essere dell'amministrazione (CARLONI). Al concetto di *open government*, dunque, è strettamente legato quello di ***collaborative democracy*** che descrive una nuova relazione tra il governo ed i cittadini che persegue il coinvolgimento di questi ultimi nel processo di *policy-making*, nell'agenda politica, nella sua esecuzione e valutazione.

In generale, la P.A. è definita come aperta quando i cittadini possono conoscere tutti i documenti, le decisioni ed i dati dell'ente. In una simile prospettiva l'accessibilità delle informazioni è strumentale all'instaurazione di un rapporto di fiducia tra istituzioni e cittadini, destinatari dei suoi interventi. Infatti, l'apertura è finalizzata a rendere chiari e comprensibili i meccanismi decisionali, a semplificare le procedure allo scopo della miglior cura dell'interesse pubblico (BOMBARDELLI). Un elevato livello di partecipazione al processo decisionale, quindi, migliora la qualità dei prodotti e dei servizi resi, incidendo sulla percezione dei cittadini nei confronti del sistema decisionale

dell'amministrazione. L'apertura, di conseguenza, diventa un elemento essenziale per l'ideazione o il miglioramento delle politiche pubbliche, in quanto una maggiore partecipazione, stimolata dalla trasparenza, porta a decisioni più democratiche e permette di controllare efficacemente l'azione amministrativa, al fine di disincentivare o ridurre comportamenti illeciti o non efficienti. Tuttavia, gli obiettivi di trasparenza, partecipazione e collaborazione non sarebbero realizzabili se non fossero messi a disposizione di tutti dati aperti, aggiornati e riutilizzabili e senza l'uso delle tecnologie informatiche.

Si ritiene che *e-gov* e *open gov* siano intimamente collegati in quanto l'applicazione delle tecnologie ICT all'azione ed all'organizzazione amministrativa influenza sensibilmente la trasformazione del rapporto tra P.A. e cittadini, nella prospettiva di un miglioramento dell'azione pubblica. Il modello su cui si basa questo approccio è quello di un sistema pubblico integrato, nel quale la dimensione digitale diventa strumento di efficienza ed apertura del sistema amministrativo e dei servizi pubblici, nonché di maggiore partecipazione alle scelte pubbliche. Merloni precisa che ogni punto della rete è un *front office*, aperto all'accesso dall'esterno; l'intera rete costituisce il *back office*, cioè il complesso integrato di dati e di informazioni che sono messi a disposizione di chi accede alla rete. L'*open government*, quindi, unisce l'utilizzo delle tecnologie informatiche all'interno dei processi amministrativi ad un processo di modifica dei rapporti tra P.A. e collettività, anche rispetto alla riorganizzazione dell'amministrazione stessa, nell'ottica di una transizione da un'amministrazione dirigistica e gerarchizzata, ad una basata sul consenso. Ciò contribuisce, in definitiva, all'intensificarsi del confronto e della cooperazione tra soggetti pubblici e privati che concorre, a sua volta, a realizzare una società più aperta e democratica. L'*open gov*, di conseguenza, costituisce uno strumento di modernizzazione e riforma della P.A..

2.3. I principi dell'*open government*: trasparenza, partecipazione, collaborazione

Nel quadro della dottrina dell'o*pen government*, non solo devono essere rese disponibili le informazioni relative a tutte le attività delle P.A., ma deve essere ridefinito il rapporto tra amministrazione e privati passando da un approccio in cui il cittadino è mero fruitore delle prestazioni erogate dall'amministrazione, ad uno basato sulla collaborazione. L'**apertura** diventa centrale nell'evoluzione del sistema, in quanto rappresenta il fulcro attorno al quale ruota il **cambiamento complessivo del modello di pubblica amministrazione**, ovvero del rapporto tra istituzioni e cittadini, grazie all'uso delle tecnologie informatiche, in particolare il web 2.0, che presenta piattaforme che permettono tale tipo di interazione.

Secondo la definizione di *Open Government Partnership*, un governo che si propone di essere aperto deve garantire la trasparenza, la partecipazione e l'*accountability*. La **trasparenza** delle

informazioni è resa necessaria in quanto i cittadini devono poter accedere a tutte le informazioni volte a conoscere il funzionamento e l'operato delle pubbliche amministrazioni; ciò aiuta ad aumentare la fiducia nelle istituzioni ed a stimolare il sistema economico. La **partecipazione** di tutti i cittadini i quali, senza alcuna discriminazione, devono essere coinvolti nei processi decisionali e nella definizione delle politiche contribuendo con idee, conoscenze e abilità rivolte al bene comune e all'efficienza delle amministrazioni. L'***accountability***, ovvero l'obbligo dei governi di "rendere conto" ai cittadini del proprio operato e delle proprie decisioni, garantendo la piena responsabilità dei risultati conseguiti.

Un impulso decisivo alla diffusione di tali politiche è stato dato dall'amministrazione del Presidente statunitense **Barack Obama**. Il primo atto del suo mandato presidenziale è stato il ***memorandum*** del 21.01.2009 ai direttori dei dipartimenti e delle agenzie federali dal titolo "*Transparency and Open Government*", il quale disegnava un vero e proprio modello normativo ed organizzativo (tutti i memorandum del Presidente Obama sono disponibili sul sito obamawhitehouse.archives.gov). Tale provvedimento indicava i principi dell'*open government* alle agenzie pubbliche, assegnando loro un elenco di compiti ed una tabella di marcia da seguire. Nel modello tracciato dal memorandum presidenziale con *open government* si faceva riferimento ad un'azione amministrativa ed istituzionale improntata ai principi di **trasparenza**, **partecipazione** e **collaborazione**. Questi tre principi hanno costituito i pilastri della nuova dottrina sull'*open government* e sono stati poi seguiti anche dagli altri Stati che hanno adottato tali politiche.

Secondo il memorandum citato, per costruire un nuovo modello **l'amministrazione dovrebbe essere trasparente** (*government should be transparent*), in quanto essa **favorisce la responsabilizzazione e fornisce informazioni per i cittadini** (*transparency promotes accountability and provides information for citizens*). Le istituzioni dovrebbero tenere un'azione appropriata, sia a livello di norme che di politiche, diffondendo rapidamente le informazioni in forme che il pubblico possa trovare e utilizzare prontamente, mediante le nuove tecnologie. In altri termini, la trasparenza consente l'*accountability*, fornendo informazioni ai cittadini sull'operato della P.A.

A livello nazionale, un passaggio significativo verso un nuovo modello è dato dal Codice della Trasparenza, che lega la trasparenza ad un diverso modo di amministrare, caratterizzato dai paradigmi della buona amministrazione e dell'amministrazione aperta (art. 1 comma 2). L'impianto tradizionale del rapporto tra potere pubblico e cittadino fino a poco tempo fa era ispirato dalla teoria del segreto, secondo la quale le informazioni segrete sono tali perché la loro conoscenza danneggerebbe interessi che l'ordinamento ritiene prevalenti rispetto al diritto all'informazione. Il paradigma fondamentale del diritto pubblico del XX secolo si fondava sul paradigma bipolare, in

base al quale P.A. e privati rappresentano i due poli di un rapporto asimmetrico, conflittuale, fondato sulla separazione e la divergenza degli interessi. (ARENA). La teoria del segreto era coerente con un modello di P.A. gerarchica, nel quale il rapporto tra potere pubblico e cittadini era inteso in termini di separazione e superiorità. Per questo motivo, la conoscibilità è diventata una dei concetti chiave di riforma della P.A. che, rafforzando la posizione dei cittadini, attribuisce loro il **diritto a conoscere** (*right to know*) e sancisce il parallelo **dovere delle amministrazioni di far conoscere**, rimodulando il rapporto tra amministrazione cittadini. Nel nuovo modello, la trasparenza viene ricondotta anche al piano dell'amministrazione attiva, come principio necessario per porre le basi per un dialogo più consapevole tra P.A. e cittadini (BOMBARDELLI).

Secondo il memorandum di Obama **l'amministrazione dovrebbe essere partecipativa**, con lo scopo di **coinvolgere i cittadini nelle decisioni amministrative** rendendo l'operato dei pubblici poteri più efficace e, di conseguenza, migliorare la qualità delle decisioni. Secondo il memorandum le conoscenze sono ampiamente disperse nella società e i pubblici ufficiali traggono vantaggio dall'avere accesso ad esse; per questo motivo, le P.A. dovrebbero offrire ai cittadini maggiori opportunità per partecipare al processo decisionale ed al governo con i benefici della propria esperienza e delle proprie conoscenze collettive (*opportunities to participate in policymaking and to provide their Government with the benefits of their collective expertise and information*). Favorire i processi partecipativi, infatti, è utile in primo luogo alle istituzioni, perché agevola l'assunzione di decisioni corrette, dal momento che consente di acquisire idee e competenze (*ideas and expertise*) che permettono di sviluppare politiche migliori.

La **partecipazione** è, quindi, da intendere sia come **apertura all'intervento dei cittadini**, sia come **rapporto collaborativo con altri soggetti pubblici**. Seguendo questo paradigma si passa da un modello di amministrazione autoritativo e gerarchico ad un modello di tipo inclusivo, ovvero a moduli che prevedono, favoriscono e utilizzano l'intervento dei cittadini, sia singoli che riuniti in associazioni. In tale processo di cambiamento dell'impianto del potere pubblico l'apporto del cittadino diventa centrale, in quanto egli viene considerato protagonista delle decisioni pubbliche in ragione della sua interazione e collaborazione con le amministrazioni. Il coinvolgimento dei cittadini può avvenire attraverso vari strumenti e modalità, ad esempio le conferenze di servizi o gli accordi di programma; a tale scopo un ruolo essenziale viene riconosciuto all'utilizzo delle tecnologie, in quanto la loro capacità interattiva permette di partecipare a procedimenti nei quali, in loro assenza, sarebbe stato difficile intervenire. La interattività delle tecnologie favorisce il coinvolgimento di esperti, associazioni e soggetti interessati ad una certa decisione, permettendo loro di intervenire nel dibattito su di essa, oltre a favorire una più ampia conoscenza delle situazioni locali. Dall'altro lato, la partecipazione degli interessati costringe la P.A. a motivare le sue scelte,

rendendo difficile l'indifferenza dei soggetti istituzionali ai suggerimenti pervenuti (RODOTÀ).
Attraverso la partecipazione, in definitiva, si costruisce un modello di democrazia partecipativa e collaborativa, in cui il cittadino partecipa alle scelte di governo relative ad interessi generali (sussidiarietà orizzontale) (DE TOFFOL, VALASTRO), favorendo la partecipazione di soggetti altrimenti esclusi dalle istituzioni rappresentative classiche e favorendo, allo stesso tempo, la distribuzione delle funzioni tra i vari livelli di governo (sussidiarietà verticale).
L'amministrazione, infine, **dovrebbe essere collaborativa** (*government should be collaborative*); la **collaborazione coinvolge attivamente i cittadini nel lavoro delle amministrazioni**, le quali dovrebbero utilizzare strumenti, metodi e sistemi innovativi per cooperare tra loro, a tutti i livelli di governo e con organizzazioni non profit, imprese e individui nel settore privato. Infatti, rivedere i modelli organizzativi garantisce la costante collaborazione tra i vari attori sociali. Le istituzioni, inoltre, dovrebbero sollecitare un *feedback* pubblico per valutare e migliorare il loro livello di collaborazione e identificare nuove opportunità di cooperazione (*innovative tools, methods, and systems to cooperate among themselves, across all levels of Government, and with nonprofit organizations, businesses, and individuals in the private sector. Executive departments and agencies should solicit public feedback to assess and improve their level of collaboration and to identify new opportunities for cooperation*).
La collaborazione, inoltre, è da intendersi quale **meccanismo di raccordo tra gli altri due pilastri** *dell'open government*, ossia trasparenza e partecipazione. La collaborazione riduce ulteriormente lo spazio riconosciuto alla visione dell'amministrazione come soggetto portatore di interessi contrapposti, antagonisti, rispetto a quelli dei cittadini, elevando la partecipazione ad un altro livello. I cittadini possono utilmente contribuire a modellare l'agenda delle istituzioni ed esprimere le loro opinioni sulle alternative politiche definite in anticipo; essi possono anche concorrere a determinare gli strumenti e i metodi con cui vengono perseguiti gli obiettivi di politica pubblica (CARLONI). Se l'amministrazione è collaborativa, i cittadini diventano una risorsa, contribuendo sia all'identificazione che al perseguimento di obiettivi pubblici.

2.4 *Open data*

Il cambiamento di paradigma nel rapporto tra amministrazione e cittadini si muove sul terreno dell'informazione, che riconosce la rilevanza dei **dati e delle informazioni** come **presupposto delle decisioni pubbliche**. Senza la disponibilità di dati, documenti e informazioni non sarebbe possibile rendere effettivo il modello dell'*open government*.
Se la trasparenza amministrativa, intesa come il diritto a conoscere ma anche a comprendere ciò che si è conosciuto (ARENA) acquista un ruolo fondamentale per lo sviluppo della democrazia, i cittadini

devono poter utilizzare le informazioni detenute dalle P.A. per formarsi un'opinione, sulla base della quale poi operare delle scelte. Per dare **attuazione ai principi** di trasparenza, partecipazione e collaborazione occorre fornire al cittadino gli **elementi conoscitivi necessari per poter fare scelte e valutare le decisioni prese dalle istituzioni pubbliche**. Il modello dell'amministrazione condivisa si lega, dunque, all'utilizzo da parte di cittadini delle potenzialità conoscitive dei dati di provenienza pubblica, diffusi in formato aperto, completi, aggiornati e suscettibili di riutilizzo, cioè senza restrizioni di *copyright* o altre forme di controllo che ne limitino la riproduzione.

In questa prospettiva, l'insieme dei dati in possesso delle P.A. costituisce un giacimento conoscitivo, che si distingue dalle altre fonti per la qualità e quantità dei dati che lo compongono. L'*open data* può essere letto in rapporto di complementarità rispetto ai principi dell'*open government* (PONTI), in quanto la disponibilità di informazioni consente forme di collaborazione e di rielaborazione della conoscenza. Di conseguenza aprire i dati alla disponibilità dei cittadini è un fattore di sviluppo, sia democratico che economico, delle società contemporanee.

Un **dato** può definirsi il **mezzo su cui viaggia un'informazione elementare**. Il valore dei dati grezzi aumenta sensibilmente quando questi vengono incrociati, dal momento che la loro combinazione è in grado di restituire un'informazione sempre più complessa. I dati possono essere intesi come singoli pezzi di informazioni di qualsiasi natura (immagini, numeri, definizioni testuali, mappe, audio etc.) che sono descrizioni dirette di fatti o sono strettamente legate ai fatti e, come tali, non sono protetti da *copyright*, ma sono riproducibili senza ambiguità quando il metodo utilizzato per generarli è noto in tutti i suoi dettagli (FIORETTI). Secondo la definizione fornita dalla *Open Knowledge Foundation* (OKF), gli *open data* "possono essere liberamente utilizzati, riutilizzati e redistribuiti, con la sola limitazione della richiesta di attribuzione dell'autore e della redistribuzione allo stesso modo". Si passa quindi dalla libera accessibilità dei dati della P.A. alla libera condivisione e riutilizzazione degli stessi da parte di soggetti terzi.

Secondo il paradigma tracciato dal Presidente Obama, infatti, il dato diventa "aperto" se, una volta pubblicato, è "*easily available to entrepreneurs, researchers, and others who can use those files to generate new products and services, build businesses, and create jobs"*. Ossia, quando diventa utilizzabile, anche per scopi commerciali. L'*open data* è funzionale al settore privato, in quanto costituisce una risorsa per la crescita economica e la creazione di posti di lavoro. I dati, infatti, avendo un valore intrinseco, possono essere rielaborati e combinati in modo creativo da privati, istituti di ricerca ed imprese. Le amministrazioni quindi devono pubblicare le informazioni *online*, utilizzando un formato aperto che possa essere leggibile dagli elaboratori e reso disponibile al pubblico in modo che sia permesso il riuso dell'informazione veicolata. In altri termini, l'*open data* punta a stimolare l'utilizzo delle informazioni rese disponibili senza costi, con licenze aperte,

consentendone la massima utilizzazione per creare applicazioni utili ai cittadini nella loro vita quotidiana (*to create applications useful to citizens in their everyday lives*).

Nello svolgimento delle loro attività istituzionali le pubbliche amministrazioni producono, raccolgono, organizzano numerose informazioni che possono essere il risultato di specifiche attività di rilevazione condotte dalle stesse, come il catasto, oppure prodotte nell'adempimento di specifici obiettivi. Spesso tali informazioni interessano il cittadino, in quanto sono riutilizzabili per finalità conoscitive diverse, al punto che si può parlare di interesse pubblico; per questo motivo l'accesso a tali informazioni dovrebbe essere riconosciuto come un diritto, secondo il principio per cui i cittadini sono i proprietari ultimi dei dati, oltre ad essere la fonte primaria delle indagini e delle raccolte. Alla base della dottrina *open data*, in altri termini, sta la considerazione per cui i dati prodotti dalle P.A. in quanto finanziati da denaro pubblico devono ritornare ai contribuenti – e alla comunità in generale – sotto forma di dati aperti e universalmente disponibili.

Parte dagli stessi presupposti anche la Carta dei Dati Aperti del G8 (*Open Data Charter*, del giugno 2013), in base alla quale "l'accesso ai dati consente agli individui e alle organizzazioni di sviluppare nuove idee e innovazioni che possono migliorare le vite degli altri e aiutare a ridurre il flusso delle informazioni all'interno e tra gli Stati". Nell'ottica della Carta i principi che guidano l'apertura dei dati sono la trasparenza e la creazione di valore attraverso i dati aperti, il cui utilizzo può portare allo sviluppo di nuove applicazioni, anche mischiando dati provenienti da fonti diverse (*mash-up*).

Il **Codice dell'Amministrazione Digitale**, nella versione seguita all'ultima modifica (avvenuta con il d.lgs. n. 217/2017) definisce all'**articolo 1 comma 1 lett. l-bis**) il **formato aperto** come un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi; la successiva **lettera l-ter**) definisce le **caratteristiche** dei dati di tipo aperto, i quali devono essere resi disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato. I dati devono essere accessibili attraverso le tecnologie ICT, ivi comprese le reti telematiche pubbliche e private, in formati aperti adatti all'utilizzo automatico da parte di programmi per elaboratori. I dati, infine, devono essere resi disponibili gratuitamente.

Il legislatore ha affrontato il tema sia nel quadro della disciplina dell'amministrazione digitale, sia in quella dell'*open data government*, in particolare nel **Codice della Trasparenza**, che è stato emanato in attuazione della delega contenuta nella legge anticorruzione relativa all'obbligo di pubblicare gli atti, i documenti e le informazioni soggetti a regime di pubblicità obbligatoria in formato elettronico, elaborabile e in formati di dati aperti (art. 35 comma 1 lett. f) legge n. 190/2012). Il Codice, all'**articolo 1 comma 1,** prevede che **la trasparenza debba essere intesa**

come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. **L'articolo 6** prevede che **le amministrazioni garantiscano la qualità delle informazioni** assicurandone l'integrità, l'aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, l'accessibilità, nonché la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità.

Il successivo **articolo 7** dispone **che i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria siano pubblicati in formato di tipo aperto**, secondo la disciplina del CAD e siano riutilizzabili. L'**articolo 7 bis** (introdotto dall'art. 7 del d.lgs. n. 97/2016) chiarisce, poi, che gli obblighi di pubblicazione dei dati comportano la possibilità della loro diffusione attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo, fermo restando il rispetto dei principi sul trattamento dei dati personali.

Al Capo II sono elencati, infine, i dati e le informazioni che le P.A. devono rendere disponibili obbligatoriamente tra i quali quelli relativi all'organizzazione, quelli concernenti i titolari di incarichi politici, di amministrazione, di direzione o di governo e i titolari di incarichi dirigenziali, o i titolari di incarichi di collaborazione o consulenza.

3. Le norme dell'amministrazione aperta nel Codice dell'Amministrazione Digitale

3.1. L'evoluzione della disciplina ed i principi fondamentali

La digitalizzazione dei servizi e l'ammodernamento del settore pubblico si sviluppa attraverso politiche e normative riconducibili all'agenda digitale italiana ed europea. Il CAD non si limita a contenere la disciplina organica degli strumenti telematici di interazione tra cittadini e P.A., ma prevede l'obbligo per le amministrazioni dell'uso delle tecnologie informatiche, attribuendo a cittadini e imprese il corrispondente diritto di pretendere la reciprocità digitale (BELISARIO, COSTANTINO).

Nel percorso verso la digitalizzazione della P.A. la legge n. 124/2015 (legge Madia) ha avuto un ruolo di rilievo, legando esplicitamente il tema della digitalizzazione a quello della semplificazione. Particolarmente significativi sotto questo punto di vista sono il decreto legislativo n. 179/2016, il successivo correttivo, d.lgs. n. 217/2017, ed il d.lgs. n. 97/2016. Quest'ultimo, modificando il d.lgs. n. 33/2013 e la legge n. 190/2012, ha introdotto nel nostro ordinamento il principio dell'accessibilità totale agli atti e ai documenti delle amministrazioni. L'**articolo 1 della legge Madia** è intitolato

“**Carta della cittadinanza digitale”** e prevede la delega al Governo a riformare il CAD con uno o più decreti, allo scopo di “garantire ai cittadini e alle imprese il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale”. Obiettivo dichiarato della riforma è quello di semplificare “l'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici”. La riforma è avvenuta in due momenti, il primo passo ha comportato l’adozione del d.lgs. n. 179/16 e il secondo è stato compiuto con il correttivo del 13.12.2017, adottato per migliorare le disposizioni in materia di amministrazione digitale, che completa le riforme al Codice.

La scelta di dedicare ai diritti di cittadinanza digitale l’articolo 1 della legge è sintomatica della centralità riconosciuta alle tecnologie ICT nei rapporti tra cittadini, imprese e pubbliche amministrazioni, quale strumento per la promozione del processo di riorganizzazione dell’amministrazione. Nell’ottica del legislatore la digitalizzazione è funzionale a garantire ai cittadini il diritto di accedere non solo ai dati e documenti, ma anche ai servizi. Il d.lgs n. 97/2016 riconosce la centralità delle tecnologie digitali nei rapporti tra cittadini, imprese e amministrazioni quale strumento di innovazione e sposta l'attenzione dal processo di digitalizzazione delle amministrazioni alla cittadinanza digitale e ai diritti di cittadini e imprese. La delega al Governo a intervenire sulla disciplina contenuta nel CAD è stata attribuita allo scopo di promuovere e rendere effettivi i diritti di cittadinanza digitale. Con la “Carta della cittadinanza digitale” i diritti sono stati riconosciuti direttamente a cittadini e imprese, superando la complessità della situazione precedente per cui ogni amministrazione o ente pubblico richiedeva proprie modalità di registrazione e di utilizzo per la fruizione dei servizi *online*. La legge ha imposto di semplificare il CAD in modo da contenere esclusivamente principi di carattere generale, che garantiscano un livello minimo di tutela. Sotto il profilo del metodo è stata realizzata un’ampia consultazione della società civile; si è trattato di un esempio concreto ed effettivo di *open government*, che ha visto il coinvolgimento di soggetti esperti di diversa provenienza.

Dal testo definitivo del Codice emerge in modo chiaro la volontà di proseguire nella direzione di una **modernizzazione, attraverso la leva dell’innovazione digitale** della pubblica amministrazione. L’intento del legislatore è quello di favorire un’interazione digitale e semplice tra cittadini e amministrazioni, anche ampliandone l’**ambito soggettivo di applicazione** (**articolo 2**). Fino al decreto del 2016 il CAD si applicava solo alle P.A. in senso stretto (comuni, province, ministeri, città metropolitane, scuole, etc); la riforma del 2016 aveva previsto l’estensione alle società controllate e partecipate, mentre con il correttivo del 2017 è stata prevista l’estensione ai gestori dei servizi pubblici. Si tratta di un’estensione significativa nell’ottica di una maggiore trasparenza e di un più efficace controllo pubblico, in quanto ovunque ci sia impiego di denaro

pubblico deve essere applicato il Codice come misura di controllo della spesa, considerando la natura intrinseca della digitalizzazione, che comporta dei risparmi. Inoltre, ovunque vi siano servizi pubblici, indipendentemente dal soggetto che li eroga, vi devono essere degli standard minimi da rispettare per i servizi all'utente.

Il Codice è considerato una delle regolazioni centrali per l'affermazione di un nuovo modello di relazione tra P.A. e cittadini, sebbene il principio del ricorso alle tecnologie informatiche nelle relazioni tra questi due soggetti sia stato inserito dalla legge n. 15/2005 nella legge n. 241/90 (LPA) con l'art. 3 bis. Vi è un legame tra l'art. 3 bis LPA e l'art. 12 comma 1 del Codice. L'art. 3 bis impone alle P.A. di incentivare l'uso della telematica per rendere più efficiente la loro attività. L'art. 12 comma 1 CAD descrive la digitalizzazione come un fattore di modernizzazione e trasformazione della P.A., prevedendo il ricorso alle ICT per realizzare obiettivi efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese. In base ad una lettura combinata dei due articoli i principi che regolano l'azione amministrativa beneficiano dell'uso della tecnologia che implica, per ciò solo, la possibilità di una maggiore e migliore partecipazione dei privati all'azione amministrativa. Infatti, le tecnologie informatiche devono essere legate ad un cambiamento organizzativo e nell'acquisizione di nuove competenze, in modo da migliorare i servizi pubblici e il processo democratico e sostenere le politiche pubbliche (MERLONI).

Per rendere effettivi i principi dell'*open government*, dunque, nel Codice si afferma il **principio di disponibilità dell'informazione in formato digitale** (**art. 2 comma 1**) ponendo allo Stato, alle Regioni ed alle autonomie locali il dovere di assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale. L'**articolo 3** introduce il **diritto all'uso delle tecnologie nei rapporti con i soggetti pubblici**; nella versione risultante dal correttivo del 2017 si specifica che, anche ai fini della partecipazione al procedimento amministrativo, chiunque ha il diritto di usare in modo accessibile ed efficace le soluzioni e gli strumenti.

3.2. Trasparenza e *open data*

Il primo pilastro dell'*open government* è dato dalla trasparenza e *open data*. Il disegno normativo, così come risultante dalle recenti modifiche, va nel senso del potenziamento della connessione e della creazione di flussi comunicativi stabili fra le diverse amministrazioni e fra queste ed i cittadini, in quanto la comunicazione viene considerata irrinunciabile per garantire il pieno conseguimento degli obiettivi di interesse generale che alle P.A. sono affidati. La trasparenza

permea l'intero CAD ed il principio risulta accentuato attraverso l'estensione delle possibilità di controllo democratico dei cittadini. Il controllo è realizzato utilizzando le **tecnologie informatiche come mezzo privilegiato per la diffusione delle informazioni**, aumentando i contenuti che le P.A. devono pubblicare obbligatoriamente sul web. In tal senso vanno letti gli artt. 12 comma 2 e 54 del Codice.

Il Codice adotta un criterio di interconnessione che impone a ogni P.A. di assicurare sia alle altre pubbliche amministrazioni che ai privati, la disponibilità, la pubblicità, l'accessibilità e la fruibilità dei dati. La disciplina positiva, dunque, considera le potenzialità dell'informatica non solo sul piano quantitativo, come strumenti per rendere più veloci gli schemi procedimentali esistenti, ma anche sul piano qualitativo, come strumento per impostare nuovi modelli procedurali, più semplici, completi e dinamici. Oltre alle norme contenute nel d.lgs. n. 33/2013, – che ha introdotto il FOIA (*freedom of information act*) sulla base del modello statunitense – sul punto sono fondamentali le previsioni di cui agli artt. 3 e 41 e quelle contenute nel Capo V del CAD, intitolato proprio ai dati pubblici. L'art. 3, come visto, prevede il diritto all'uso delle tecnologie, mentre l'art. 41 dispone che le P.A. gestiscano in via prioritaria i procedimenti amministrativi tramite strumenti informatici, fornendo i servizi di interoperabilità o integrazione.

Un vero e proprio **statuto della trasparenza tramite gli *open data*** è contenuto nell'**articolo 50**, il quale afferma che i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie informatiche che ne consentano la fruizione e riutilizzazione. La disposizione ha permesso di realizzare un effettivo *open government* e costituisce il secondo tassello normativo, che sviluppa e arricchisce il principio di disponibilità dei dati e delle informazioni, di cui all'art. 2, riconoscendo un ruolo fondamentale ai dati digitali, i quali diventano centrali come informazioni di base. Il legislatore completa il principio di disponibilità esplicitandone la finalità, che è quella di consentire la fruizione dei dati di cui ogni P.A. è titolare da parte di altre amministrazioni e la riutilizzazione da parte dei privati e delle amministrazioni. Il Codice considera i dati una risorsa primaria al fine di raggiungere una maggiore trasparenza, dal momento che la loro consultazione permette di ottenere una visione globale ma, allo stesso tempo, anche analitica di una certa situazione amministrativa. Per questo motivo riconosce alla generalità degli interessati l'accessibilità, il riutilizzo e fruizione gratuita e senza necessità di identificazione informatica.

Il correttivo del 2017 ha modificato l'art. 50 aggiungendovi il **comma 2-bis**, il quale prevede che le pubbliche amministrazioni nell'ambito delle proprie funzioni istituzionali procedano all'analisi dei propri dati anche in combinazione con altre amministrazioni (o gestori di servizi pubblici per profili di pubblico interesse o società a controllo pubblico), secondo le linee guida dell'Agenzia per l'Italia

Digitale (AgID). In particolare le linee guida dovranno chiarire gli aspetti tecnologici del funzionamento dei modelli di cooperazione applicativa, allo scopo di valorizzare il patrimonio informativo pubblico. Attraverso la diffusione della conoscenza delle informazioni, il legislatore mira a rendere effettiva la partecipazione dei privati all'azione amministrativa. Il cospicuo patrimonio informativo pubblico grazie alle nuove tecnologie può circolare ed essere rielaborato, consentendo ai privati di controllare l'operato pubblico e di produrre nuova ricchezza immateriale.

Contribuiscono a rendere effettivi tali principi le politiche relative ai dati aperti, di cui all'**articolo 52**, che stabilisce il **principio del "*open by default*"**, sancendo il passaggio verso l'apertura per le amministrazioni pubbliche. La norma prevede che quando i soggetti tenuti all'osservanza del Codice pubblicano dati e documenti, questi devono intendersi di tipo aperto, ovvero rilasciati con licenze che consentano il riutilizzo, anche per finalità commerciali, salvo l'unico obbligo di citare la fonte. L'ultimo correttivo contiene una previsione significativa, in quanto stabilisce che anche i capitolati ed i contratti che comportino la raccolta e la formazione di dati e documenti da parte della P.A. devono prevedere delle clausole che garantiscano il riutilizzo dei dati e dei documenti, in conformità a quanto previsto dall'articolo 50.

Di fondamentale rilievo è la responsabilità dell'amministrazione, sancita sempre dall'art. 52, nell'aggiornare, divulgare e permettere la valorizzazione dei dati pubblici secondo principi di *open government*. Infatti, il **comma 4** significativamente prevede che le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle P.A. rientrino tra i parametri di **valutazione della performance dirigenziale**. Inoltre, si affida all'amministrazione il compito di promuovere progetti di elaborazione e diffusione dei dati, anche attraverso l'uso del *project financing*, assicurando la gratuità dell'accesso e la pubblicazione in formato aperto, così da permettere la rielaborazione anche da parte di soggetti terzi. Significativa è anche la previsione di cui all'**articolo 51**, dedicato alla sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle amministrazioni, dal momento che non può esservi un pieno sviluppo dell'*open data* se non è possibile utilizzare i dati in piena sicurezza. La norma prevede che AgID, mediante regole tecniche, curi la **sicurezza dei dati** individuando le soluzioni tecniche idonee a garantire la protezione, l'accessibilità, l'integrità e la riservatezza dei dati, nonché la continuità operativa dei sistemi e delle infrastrutture.

Il d.lgs. n. 217/2017 ha disposto l'inserimento nel corpo del Codice dell'**art. 50 ter**, rubricato "Piattaforma Digitale Nazionale Dati". Il legislatore delegato intende promuovere la progettazione, lo sviluppo e la sperimentazione di una **Piattaforma Digitale Nazionale Dati finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo** detenuto per finalità istituzionali dai soggetti tenuti all'applicazione del Codice, salvo specifiche esclusioni previste dalla norma. La piattaforma, inoltre, dovrà favorire la condivisione dei dati tra i soggetti che hanno diritto ad

accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese. In altri termini, la Piattaforma ha il fine di favorire la condivisione dei dati fra le pubbliche amministrazioni, di semplificare l'accesso ai dati stessi da parte dei soggetti che hanno diritto ad accedervi e di semplificare gli adempimenti e gli oneri amministrativi per i cittadini e le imprese. Questa ultima previsione è funzionale non solo ad implementare il livello di trasparenza, ma anche a favorire la partecipazione dei cittadini e la collaborazione tra amministrazioni, dal momento che la condivisione dei dati e la semplificazione dell'accesso agli stessi permettono un più agevole – e dunque efficace – utilizzo del patrimonio informativo pubblico. In ultimo, sul punto occorre ricordare le linee guida di AgID sulla valorizzazione del patrimonio informativo pubblico, che definiscono standard e criteri per la pubblicazione di dati aperti e per la definizione delle strategie delle P.A. Tali linee guida mirano a fornire indicazioni puntuali sui passi da seguire per creare un processo standardizzato di gestione del dato aperto presso le amministrazioni.

L'**interoperabilità**, ovvero **la capacità di combinare una base di dati con altre** è essenziale per la creazione di sistemi sofisticati di utilizzo di questi, dal momento che permette a componenti diverse di lavorare insieme. Gli insiemi di dati accessibili e utilizzabili in modo condiviso, potenzialmente possono essere "mescolati" con dati provenienti da altre fonti aperte; da questo punto di vista l'interoperabilità è la chiave per realizzare il principale vantaggio pratico dell'apertura per sviluppare nuovi e migliori prodotti e servizi. In particolare, per i cittadini il riutilizzo offre la possibilità di una migliore informazione e conoscenza delle attività delle istituzioni, di fatto rendendole più trasparenti, mentre favorisce la collaborazione tra le P.A., in quanto permette un risparmio dei costi e l'interoperabilità dei sistemi.

Il legislatore, consapevole del fatto che riutilizzo delle informazioni del settore pubblico comporta una serie di vantaggi per la collettività, lo ha disciplinato. Il CAD contiene alcune norme volte a razionalizzare gli strumenti di coordinamento e collaborazione delle amministrazioni pubbliche per conseguire risparmi di spesa, anche favorendo l'*open source*. **L'articolo 69** dispone che le amministrazioni titolari di soluzioni e programmi informatici hanno l'obbligo di rendere disponibile il relativo codice sorgente (corredato dalla documentazione e dalla relativa descrizione tecnico funzionale), completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni previste dalla stessa norma.

L'articolo 60, invece, ha per oggetto le **basi di dati di interesse nazionale**, quale insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni. Il comma 1 definisce base di dati di interesse nazionale come l'insieme delle informazioni raccolte e gestite digitalmente dalle amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è rilevante per lo

svolgimento delle funzioni istituzionali delle altre P.A., anche solo per fini statistici. Le basi di dati costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle amministrazioni interessate. Tali sistemi informativi, secondo la norma, devono possedere alcune caratteristiche minime di sicurezza, accessibilità e interoperabilità. Con la modifica operata dall'ultimo correttivo sono stati introdotti due nuovi commi (2-*bis* e 2-*ter*) che contengono norme significative anche nell'ottica di favorire la collaborazione tra i soggetti pubblici, secondo i canoni dell'*open government*. Si prevede che le amministrazioni responsabili di tali basi di dati debbano consentire il pieno utilizzo delle informazioni ai soggetti di cui all'articolo 2, comma 2 secondo standard e criteri di sicurezza e di gestione definiti nelle linee guida di AgID, oltre a definire e pubblicare i piani di aggiornamento dei servizi per l'utilizzo delle medesime basi di dati.

Il Correttivo, inoltre, ha modificato il comma 3-*ter* il quale, nella sua attuale formulazione, prevede che AgID pubblichi sul proprio sito istituzionale l'elenco delle basi di dati di interesse nazionale. Secondo la novella, nello svolgere tale compito l'Agenzia individua le basi di dati di interesse nazionale, tenendo conto delle esigenze delle amministrazioni e degli obblighi derivanti dai regolamenti europei. Nell'ambito del Piano Triennale per l'informatica nella P.A. (2017-2019) sono state identificate una serie di basi di dati di interesse nazionale. La lista fornita non è esaustiva ma riporta le basi di dati di interesse nazionale come attualmente indicate nel Codice e in altre norme di riferimento, nonché un insieme di basi di dati equiparabili a quelle di interesse nazionale.

3.3. Partecipazione e collaborazione

Gli altri principi tradizionali dell'*open government* sono legati alla partecipazione e alla collaborazione. Il Codice contiene varie previsioni rilevanti sul punto.

L'articolo 8, così come modificato dal d.lgs. n. 179/2016 contiene una norma di rilievo, imponendo alle amministrazioni di promuovere **iniziative volte a favorire la diffusione della cultura digitale tra i cittadini**, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle P.A. con azioni specifiche e concrete. La previsione è volta a stimolare la crescita delle competenze digitali dei cittadini, essenziali per poter utilizzare in modo pieno e corretto i servizi digitali, ciò in quanto se i cittadini non possiedono le competenze necessarie per poter usufruire dei servizi messi a disposizione dalle P.A., i dati non possono esercitare la loro funzione di strumenti di trasparenza e partecipazione. In questo senso potremmo provare ad attribuire alle iniziative volte alla diffusione della cultura digitale la qualifica di una nuova educazione civica, in quanto la promozione delle competenze digitali è funzionale alla

creazione di cittadini informati e consapevoli. Diffondendo la cultura digitale si punta a permettere a chiunque un uso consapevole degli strumenti informatici, affinché possa conoscere e valutare le politiche pubbliche intraprese da chi governa e, eventualmente, contribuire alla definizione o al miglioramento di esse. Inoltre, la **diffusione della connettività internet negli uffici e luoghi pubblici** (**articolo 8 bis**) è intesa come una misura strumentale volta a garantire l'effettività dei diritti digitali del cittadino, dal momento che la possibilità di accedere alla rete in forma gratuita, prevista per tutti gli utenti, favorisce l'accesso ai servizi *online*.

L'articolo 9, relativo alla **partecipazione democratica elettronica**, intende l'uso delle tecnologie come volto a promuovere una maggiore partecipazione dei cittadini al processo democratico, anche attraverso forme di consultazione preventiva sugli atti da adottare da parte dei soggetti pubblici. La norma è rilevante in quanto definisce il principio di consultazione in base al quale, salvo che sia diversamente stabilito, la consultazione deve essere reale e deve essere svolta utilizzando strumenti che consentono di rendere effettiva la partecipazione. In aggiunta, devono essere rimossi gli ostacoli e le disuguaglianze derivanti dal *digital divide*, cui fa riferimento il precedente art. 8.

Il Governo, nell'esercizio del potere legislativo delegato, ha previsto che l'uso delle tecnologie sia strumentale a migliorare la qualità degli atti amministrativi anche attraverso l'utilizzo di forme di consultazione preventiva per via telematica sugli schemi di atto da adottare. La previsione punta a stimolare la partecipazione dei cittadini alle decisioni politiche. La norma pone l'accento su una partecipazione non meramente strumentale al miglioramento dei servizi, ma anche di scelta politica, quale quella sui modi dell'intervento pubblico. Affermando che l'uso delle tecnologie deve servire a migliorare la qualità degli atti amministrativi, si punta ad incentivare la partecipazione dei cittadini al processo decisionale dell'amministrazione al fine di ottenere il risultato che l'atto raggiunga più efficacemente lo scopo per il quale viene emanato. Sul punto il ministro Madia ha licenziato una direttiva (n. 2/2017, in G.U. n. 163 del 14/7/2017) che contiene linee guida sulla consultazione e rientra nell'*Action Plan* italiano per l'*open government*. Le linee guida definiscono una serie di principi su metodologia, strumenti, tempi e organizzazione dei processi di consultazione e sono state adottate alla fine di un iter di consultazione, in particolare con le organizzazioni della società civile dell'*Open Government Forum*, costituito all'interno del Dipartimento della Funzione Pubblica del Ministero per la Semplificazione e la Pubblica Amministrazione.

L'art. 9, inoltre, assume una portata ancor più incisiva se letto congiuntamente agli artt. 3 e 7, i quali fanno riferimento al diritto del cittadino ad interagire attraverso le nuove tecnologie con le P.A. (art. 3) ed al diritto a servizi *online* semplici e integrati (art. 7). In particolare l'articolo 7, nella versione così come modificata dal correttivo del 2017, riconosce a chiunque il diritto di fruire dei servizi erogati dai soggetti pubblici in forma digitale e in modo integrato tramite gli strumenti

telematici, anche attraverso dispositivi mobili.

La digitalizzazione non ha solo delle ricadute a livello tecnico, ma comporta – come detto – una generale riorganizzazione ed un cambiamento del modo di agire della P.A. A questo principio si ispira la norma di cui all'**articolo 15**, intitolato **digitalizzazione e riorganizzazione**, che indirizza l'azione amministrativa verso un coordinamento funzionale. Il **comma 1 stabilisce** una riorganizzazione strutturale e gestionale anche attraverso il migliore e più esteso utilizzo delle tecnologie informatiche nell'ambito di una strategia coordinata che garantisca lo sviluppo coerente del processo di digitalizzazione. In base al **comma 2** la razionalizzazione e la semplificazione hanno ad oggetto i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese. L'uso della digitalizzazione impone, quindi, il ricorso a moduli procedimentali standardizzati tra P.A., allo scopo di garantire l'interconnessione e la interoperabilità dei sistemi. Questa, di conseguenza, comporta la semplificazione e la standardizzazione dei procedimenti, resa necessaria dall'esigenza di rispettare regole tecniche comuni. Nell'intento del legislatore, in altri termini, la digitalizzazione dovrebbe tradursi in un fattore di maggiore efficienza in quanto il ricorso a modelli comuni comporta il trattamento omogeneo di situazioni similari, senza disparità legate alle scelte delle singole amministrazioni.

I principi di interconnessione ed interoperabilità, dunque, risultano funzionali allo sviluppo dell'amministrazione aperta in quanto garantiscono la cooperazione amministrativa. Il legislatore ha definito all'**articolo 1 lett. ad)** l'**interoperabilità** come la capacità di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi; alla **lettera ae)** ha definito la **cooperazione applicativa** come la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informativi dei soggetti partecipanti per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi.

Il 08.05.2018 AgID ha aperto la consultazione sulle Linee Guida Modello di Interoperabilità per le pubbliche amministrazioni, in attuazione di quanto previsto dal punto b) del comma 3-ter dell'art. 73 CAD. Il Modello di Interoperabilità è di supporto alla strategia di interoperabilità e cooperazione tra le P.A. che, definendo i contesti di interazione e integrazione tra i soggetti pubblici, i cittadini e le imprese mira a far diventare la P.A. sua interezza un unico sistema informativo virtuale. La definizione di un Modello di interoperabilità è essenziale per lo sviluppo Sistema informativo pubblico in quanto assicura l'interazione e lo scambio di informazioni tra le P.A. senza necessità di integrazioni; in tal modo si garantisce la piena collaborazione tra le amministrazioni pubbliche e i soggetti privati. La definizione del Modello di Interoperabilità risponde all'esigenza di armonizzare

la disciplina nazionale al nuovo *European Interoperability Framework* (EIF) oggetto della Comunicazione COM(2017)134 della Commissione Europea del 23.03.2017, che si pone il fine di assicurare l'interoperabilità anche nel contesto Europeo e per l'attuazione del Digital Single Market. Gli obiettivi del nuovo Modello di Interoperabilità puntano principalmente a definire le modalità di integrazione tra le P.A. ed armonizzarne le scelte architetturali e ad individuare le scelte tecnologiche che favoriscano lo sviluppo, da parte delle P.A., cittadini e imprese, di soluzioni applicative innovative che abilitino l'utilizzo dei servizi individuati nelle Infrastrutture immateriali del Piano Triennale. Nelle linee guida si promuove l'adozione dell'approccio "API first" (*application programming interface*) al fine di favorire la separazione dei livelli di *back end* e *front end*, con logiche aperte e standard pubblici che garantiscano ad altri attori, pubblici e privati, accessibilità e massima interoperabilità di dati e servizi, oltre a promuovere standard tecnologici che soddisfino l'esigenza di rendere sicure le interazioni tra le P.A. e tra queste con i cittadini e le imprese. In ultimo, esse si pongono l'obiettivo semplificare le procedure di scambio di servizi tra le P.A. e tra P.A. e privati.

Di rendere effettivi i principi ricordati *supra* si occupa l'**articolo 12 comma 2**, come modificato dal d.lgs. n. 179/2016 il quale prevede che le amministrazioni utilizzino nei rapporti interni, in quelli con altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche di cui all'art. 71. Nella medesima direzione deve essere letto l'**articolo 41 comma 1**, in base al quale le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie informatiche e, per ciascun procedimento di loro competenza, esse forniscono servizi di interoperabilità o integrazione ai sensi degli artt. 12 e 64 bis. Quest'ultimo, dopo l'ultimo correttivo, disciplina l'accesso telematico ai servizi delle P.A. prevedendo che queste debbano rendere fruibili i propri servizi in rete, garantendo anche l'integrazione e l'interoperabilità tra i diversi sistemi e servizi. Tali norme si ritiene abbiano dato cogenza – specificandole – alle previsioni di cui all'art. 3 bis della l. n. 241/1990 nonché all'art. 3 dello stesso CAD, i quali hanno una valenza programmatoria, di principio.

L'art. 18 si occupa di costituire una **piattaforma nazionale per la *governance* della trasformazione digitale**, cioè una piattaforma **per la consultazione pubblica permanente ed il confronto con i portatori di interessi**. La riformulazione operata dal d.lgs. n. 217/2017 ha introdotto la piattaforma, che è stata istituita presso AgID, la quale ne identifica le caratteristiche ai fini dell'accessibilità. La piattaforma punta a stimolare la consultazione pubblica, al fine di porre in dialogo i portatori di interessi connessi all'attuazione dell'Agenda Digitale e farvi confluire suggerimenti qualificati di migliorie, dei quali i soggetti pubblici possano tener conto. La

piattaforma, infatti, deve essere accessibile ai portatori di interessi pubblici e privati e deve essere idonea a raccogliere suggerimenti e proposte emendative in maniera trasparente, qualificata ed efficace.

Sulla piattaforma, tra l'altro, è pubblicato il Piano Triennale per l'Informatica nella Pubblica Amministrazione – approvato con DPCM del 31.05.2017 e che sarà aggiornato periodicamente, come previsto dalla norma – così come i provvedimenti che le amministrazioni ritengano sia utile pubblicarvi (non è fatto loro obbligo), relativi all'attuazione dell'Agenda Digitale. Il Piano Triennale è il documento di indirizzo strategico ed economico destinato alla P.A. che orienta la trasformazione digitale del Paese, definendo le linee operative di sviluppo dell'informatica pubblica; il modello strategico di evoluzione del sistema informativo della PA; gli investimenti ICT del settore pubblico secondo le linee guida comunitarie e del Governo.

La piattaforma costituisce una novità significativa perché è prevista come strumento per la consultazione, quindi poi per la pubblicazione di tutti gli aggiornamenti del Piano Triennale (comma 3). Essa costituisce un modulo concreto ed effettivo di apertura, in quanto si promuove il metodo della consultazione per la trasformazione digitale del paese. AgID ha già iniziato a pubblicare documenti in consultazione, ad esempio ciò è avvenuto con riferimento ai provvedimenti relativi al *cloud computing*, aprendo delle consultazioni su atti importanti per gli *stakeholders*.

Tra gli interventi previsti dal CAD volti a favorire la semplificazione, la partecipazione e la collaborazione possiamo includere anche la costruzione di un'Anagrafe Nazionale della Popolazione Residente (ANPR), che costituirà una banca dati unica contenente le informazioni anagrafiche della popolazione residente (art. 62); la realizzazione e diffusione del Sistema Pubblico di gestione dell'Identità Digitale (SPID) (art. 64), ovvero un sistema aperto che permette agli utenti di accedere con un'unica identità digitale e un'unica password ai servizi *online* delle P.A. e dei privati aderenti; l'istituzione dell'Anagrafe Nazionale degli Assistiti (ANA), di cui all'art. 62 ter, che risponde all'esigenza di monitorare la spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e amministrazioni sostituendo le anagrafi e gli elenchi degli assistiti tenuti dalle singole Aziende Sanitarie Locali con un sistema informativo nazionale.

Al fine di incentivare la realizzazione delle misure di digitalizzazione e coerentemente con tali obiettivi, l'**articolo 13 comma 1 bis**, introdotto dal d.lgs. 179/2016, prevede che la **formazione dei dirigenti** abbia ad oggetto anche competenze tecnologiche, di informatica giuridica e manageriali per la transizione alla modalità operativa digitale. Infine, l'attenzione del legislatore al raggiungimento dell'accessibilità totale, allo scopo di favorire la partecipazione, è dimostrata anche da altre norme, come gli artt. 53 e 54 che riconoscono il diritto ad avere siti internet aggiornati ed

accessibili.

3.4. La *governance*

Il soggetto a cui viene affidato complessivamente il compito di realizzare gli obiettivi dell'Agenda dell'Agenda digitale italiana, in coerenza con l'Agenda digitale europea è l'**Agenzia per l'Italia Digitale,** che coordina le azioni in materia di innovazione al fine di promuovere le tecnologie ICT a supporto della pubblica amministrazione (**articolo 14 bis**). Il legislatore ha concentrato in un'unica agenzia le competenze necessarie a promuovere l'amministrazione digitale e aperta, allo scopo di dare piena attuazione al diritto all'uso delle tecnologie, di cui all'art. 3 del CAD.

L'Agenzia è stata istituita con il d.l. n. 83/2012 intitolato "Misure urgenti per la crescita del Paese", convertito con modificazioni in l. n. 134/2012 ed ha ereditato 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. Con il d.lgs. n. 179/2016 le è stato affidato (articolo 14, comma 2) il coordinamento informatico dell'amministrazione statale, regionale e locale – che prima spettava all'organo politico – oltre al compito di favorire l'adozione di infrastrutture e standard comuni che riducano i costi sostenuti dalle amministrazioni e migliorino i servizi erogati.

Nella prospettiva generale della promozione della diffusione delle tecnologie digitali, ad AgID è attribuito il compito di elaborare gli indirizzi, le regole tecniche, gli standard e le linee guida per lo sviluppo dell'interoperabilità tra i sistemi informatici della P.A. e tra questi e i sistemi dell'Unione Europea. In particolare, l'**articolo 1 lett. ff)** definisce le **linee guida** come le regole tecniche e di indirizzo adottate secondo il procedimento di cui all'art. 71. L'Agenzia, inoltre, deve assicurare l'uniformità tecnica dei sistemi informativi pubblici destinati a erogare servizi ai cittadini e alle imprese, garantendo livelli omogenei di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo (art. 14 bis CAD).

Il nuovo Codice rafforza il **ruolo dell'Agenzia nell'attuazione dei piani del governo**, ad esempio, nella definizione di regole tecniche e principi, nella stesura dell'IT *strategy* e nella sua declinazione all'interno del Piano Triennale per l'Informatica nella Pubblica Amministrazione. L'assegnazione del compito di proporre le regole tecniche ad AgID implica un rafforzamento del suo ruolo di coordinamento, anche relativamente alla gestione del rapporto con le amministrazioni sui temi relativi all'innovazione e alla modernizzazione di sistemi e servizi, sia a livello centrale che locale.

Il nuovo **articolo 14-bis**, **in combinato disposto con l'articolo 71** attribuisce alle **linee guida**

elaborate dall'Agenzia il **compito di definire le modalità attuative di numerose disposizioni del Codice aventi carattere tecnico-operativo**, attraverso un procedimento che costituisce un concreto esempio di partecipazione e di collaborazione. Il nuovo testo dell'art. 71 prevede che le linee guida siano adottate dall'AgID, previa **consultazione pubblica**, sentite le amministrazioni competenti, la Conferenza unificata e il Garante per la protezione dei dati personali nelle materie di competenza. Le linee guida divengono efficaci dopo la loro pubblicazione nell'apposita area del sito istituzionale dell'AgID e di essa ne è data notizia in Gazzetta Ufficiale, inoltre sono modificate e aggiornate con lo stesso procedimento. La formulazione finora vigente dell'art. 71 prevedeva l'adozione di regole tecniche con decreto del Ministro delegato per la semplificazione e la pubblica amministrazione, su proposta dell'AgID, di concerto con il Ministro della Giustizia e con i Ministri competenti, sentita la Conferenza Unificata e il Garante per la protezione dei dati personali nelle materie di competenza. Nel testo previgente non si faceva menzione di una consultazione pubblica mentre nel testo attuale la previsione della necessità della consultazione pubblica introduce un modello di *open government* in tema di regolamentazione.

Una norma recente sulla *governance* è quella relativa all'ufficio del **responsabile per la trasformazione digitale**, di cui all'**articolo 17**, modificata dal decreto n. 179/2016. Il decreto del 2016 ha inciso sulle strutture, semplificandone i processi decisionali e ridefinendo le attribuzioni dell'ufficio dirigenziale che le P.A. devono istituire. L'art. 17 comma 1, allo scopo di rendere l'azione più efficace, prevede la nomina di un responsabile con adeguate competenze tecnologiche e manageriali, posto alle dirette dipendenze dell'organo politico di vertice (comma 1-ter). Lo scopo della norma è quello di far incidere la spinta riformatrice del legislatore sulla struttura, per colmarne le carenze attuative della legge registrate in precedenza.

Il responsabile per la trasformazione digitale è centrale per tutti i processi di digitalizzazione ed apertura, dal momento che rientra tra i suoi compiti la transizione non solo verso una P.A. digitale, ma anche verso una P.A. aperta. Il modello scelto dalla legge è quello del responsabile per la prevenzione della corruzione e della trasparenza (art. 1 comma 7 l. n. 190/2012 così come modificato dall'art. 41 d.lgs. n. 97/2016), ovvero un soggetto che si occupi di curare gli adempimenti previsti fungendo da connettivo, pur essendo sovraordinato agli altri uffici dirigenziali. Il legislatore ha deciso di affidare a questo soggetto tutte le attività legate al passaggio dalla modalità operativa cartacea a quella digitale ed i conseguenti processi di riorganizzazione. A tale scopo la legge gli affida poteri di impulso e di coordinamento per assicurare che vengano adempiuti tutti gli obblighi che incombono sulla P.A. in materia di amministrazione digitale e aperta. Gli adempimenti affidati al responsabile non sono quindi legati solo ai profili tecnologici, ma anche e soprattutto ai profili di organizzazione che, a loro volta, sono legati alla realizzazione di

una P.A. trasparente, digitale ed aperta, di servizi facilmente utilizzabili e di qualità, conseguendo al contempo anche una maggiore efficienza ed economicità.

Il fatto che il responsabile debba occuparsi anche di curare i processi di apertura è uno dei motivi della sua centralità per una serie di previsioni, ad esempio quella sugli *open data*. Prima dell'introduzione di questa figura, infatti, non era chiaro chi, all'interno delle amministrazioni, dovesse occuparsi di coordinare i processi di apertura dei dati; il comma 1 lettera c) chiarisce che il responsabile per la transizione è il punto di riferimento per la parte relativa alle piattaforme tecnologiche, di consultazione e partecipazione delle P.A. e anche per l'apertura dei dati.

L'ultima modifica al Codice ha introdotto nel comma 1 la lettera j-bis), che affida al responsabile – tra gli altri – compiti in tema di pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'Agenda Digitale e, in particolare, con quelli stabiliti nel Piano Triennale, confermando così la centralità della figura in tema di apertura.

4. *Open Government Partenership*, i Piani di Azione e le altre iniziative a sostegno dell'*open government*

L'Italia, attenta ai temi dell'*open government* e dell'*open data*, nel 2011 è entrata a far parte *dell'**Open Government Partnership*** (OGP), un'iniziativa multilaterale di Governi per la promozione di politiche innovative che, rendendo le istituzioni pubbliche più aperte e responsabili, mira a realizzare la trasparenza della pubblica amministrazione, la lotta alla corruzione e i principi della democrazia partecipata. I Governi, sottoscrivendo la Dichiarazione sull'*open government*, si impegnano a realizzare gli obiettivi dell'OGP attraverso alcune iniziative, sintetizzate in un Piano d'Azione, il cui contenuto è stabilito in modo partecipato con la società civile che vigila anche sulla sua attuazione. Il Piano di Azione è uno degli elementi centrali *dell'Open Government Partnership*: tutti i Paesi aderenti si impegnano, infatti, a realizzare gli obiettivi dell'OGP attraverso specifiche iniziative, che possono basarsi sugli sforzi esistenti, identificare nuove azioni per completare le riforme in corso o avviare un'azione in un settore completamente nuovo. Si tratta, in altri termini, di un'iniziativa multilaterale a livello internazionale impegnata a migliorare la relazione tra cittadini e governi puntando su apertura e *accountability*.

Nel 2015, l'Italia, insieme ad altri paesi, ha firmato la "Carta Internazionale degli *Open Data"*, adottata nell'ambito dell'*Open Government Partnership* (OGP), che contiene principi, azioni specifiche e buone pratiche sull'attuazione delle strategie e politiche di *open data*. La Carta si basa su sei principi cardine (*Open by Default; Timely and Comprehensive; Accessible and Usable; Comparable and Interoperable; For Improved Governance and Citizen Engagement; For Inclusive*

Development and Innovation) e su un sistema di regole che punta a promuovere i dati aperti come guida per il raggiungimento di obiettivi di sviluppo sostenibile dei paesi.

La parte più interessante di tutta la strategia di digitalizzazione è, probabilmente, quella riguardante gli strumenti previsti per la sua messa in atto. Tra queste figurano politiche che, nell'ambito della OGP, mirano a promuovere la cultura della trasparenza nella pubblica amministrazione attraverso l'uso di tecnologie e metodi innovativi (linee guida nazionali, metodologie comuni, nuovi software, etc.). I piani di azione nazionali e le altre iniziative di governo aperto, in essi non incluse, sono principalmente il risultato di un confronto tra le amministrazioni pubbliche partecipanti e la società civile. Il loro valore normativo è solo indiretto in quanto il contesto normativo di riferimento è dato dal CAD, mentre l'attuazione delle politiche e dei programmi è rimessa a strumenti amministrativi, oppure si basa sull'attuazione volontaria da parte dei soggetti pubblici, in quanto per attuare le politiche di *open government* in Italia si è scelta la strada dell'azione amministrativa, piuttosto che dell'intervento normativo. In altri termini, l'attuazione delle politiche è rimessa all'impegno volontario delle amministrazioni che, pur in assenza di strumenti normativi coercitivi che impongano l'attuazione delle politiche, "decidono" volontariamente di svilupparle per perseguire finalità di buon andamento per aumentare la fiducia dei cittadini.

Dall'adesione all'OGP (avvenuta con lettera del Ministro per la Pubblica Amministrazione e Semplificazione il 05.09.2011) i governi italiani hanno dedicato molte azioni amministrative alla realizzazione degli obiettivi posti a livello internazionale (i Piani di Azione sono consultabili all'indirizzo open.gov.it). Il primo Piano di Azione (2012-2014), successivamente implementato e sviluppato nei piani successivi, ha avuto il merito di iniziare il nostro Paese sulla strada dell'*open government*. Il primo Piano conteneva azioni volte a favorire la trasparenza, l'integrità, la semplificazione e politiche di *open data*, nonché misure a sostegno della collaborazione e partecipazione dei cittadini nell'attuazione delle politiche pubbliche.

Tra i principali interventi di *open government* a livello nazionale figura **Soldipubblici,** un portale creato allo scopo di promuovere e migliorare l'accesso e la comprensione dei cittadini sui **dati della spesa della pubblica amministrazione**, in un'ottica di maggiore trasparenza e partecipazione; è una delle iniziative nate a seguito del d.lgs. n. 33/2013. L'attuale versione rappresenta una prima evoluzione di quella pubblicata nel dicembre 2014 e contiene i dati relativi ai pagamenti di Regioni, Aziende Sanitarie Regionali, Province e Comuni, delle amministrazioni centrali, delle camere di commercio, delle comunità montane, degli enti di ricerca, delle strutture sanitarie e delle università purché avvenuti attraverso lo strumento del mandato elettronico. **L'obiettivo è quello di garantire la piena trasparenza e permettere sia ai cittadini che alle stesse pubbliche amministrazioni l'analisi e il monitoraggio costante delle spese**. Attraverso il portale, ad esempio, è possibile

sapere quanto è costato riqualificare uno spazio pubblico, a quanto ammontano le spese di gestione di un ente o quanto si è speso per le forniture di beni o servizi.

Particolarmente significativa a tale scopo risulta l'apertura del database SIOPE (Sistema Informativo sulle Operazioni degli Enti Pubblici), avvenuta con il D.M. del 30.05.2014, adottato in attuazione di quanto stabilito dall'art. 8 comma 3 del decreto legge n. 66/2014, convertito dalla legge n. 89/2014. L'apertura dei dati relativi ai pagamenti delle pubbliche amministrazioni è una premessa indispensabile per puntare ad un miglioramento significativo della spesa pubblica non solo in termini di risparmi quantitativi, ma anche e soprattutto in termini di efficienza e qualità della spesa. SIOPE è uno strumento di rilevazione telematica per la tracciabilità dei flussi di cassa (pagamenti e incassi) di tutte le P.A. italiane, sia centrali che periferiche. La sua apertura ha permesso di avere il quadro dettagliato della spesa pubblica corrente; in tal modo si sono create le basi per un nuovo rapporto di fiducia tra cittadini ed istituzioni anche grazie alla possibilità di effettuare valutazioni e comparazioni che rendono possibile un controllo di gestione sul singolo ente. *Soldipubblici* si basa su un proprio motore di ricerca semantico che è in grado di associare ogni ente ad una specifica voce di pagamento, sulla base delle codifiche gestionali di SIOPE, e fornire l'importo speso per il mese corrente, l'andamento della spesa annuale e altri indicatori. I dati, inoltre, sono disponibili nella sezione "Sviluppatori" e possono essere scaricati e riutilizzati. In un'ottica di *open government* è possibile segnalare mancanze, errori o porre ulteriori domande attraverso una segnalazione in un'apposita sezione ("aiutaci a migliorare") attraverso la quale i *feedback* forniti dagli utenti vengono utilizzati a supporto del monitoraggio della qualità del servizio e della risoluzione di eventuali problemi.

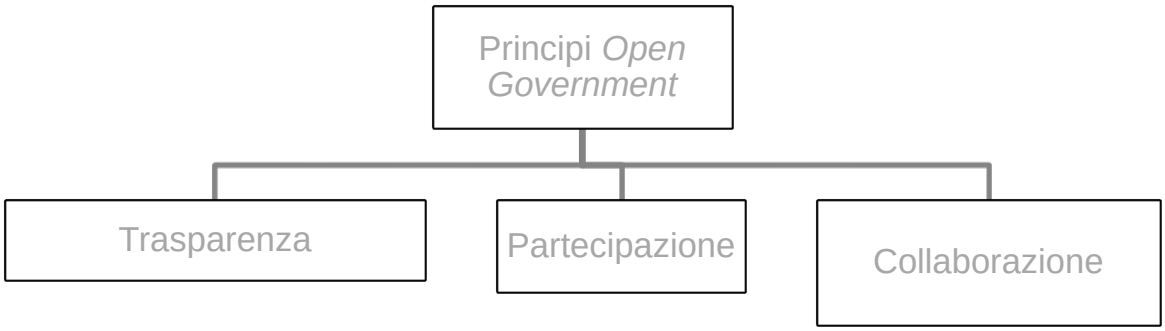
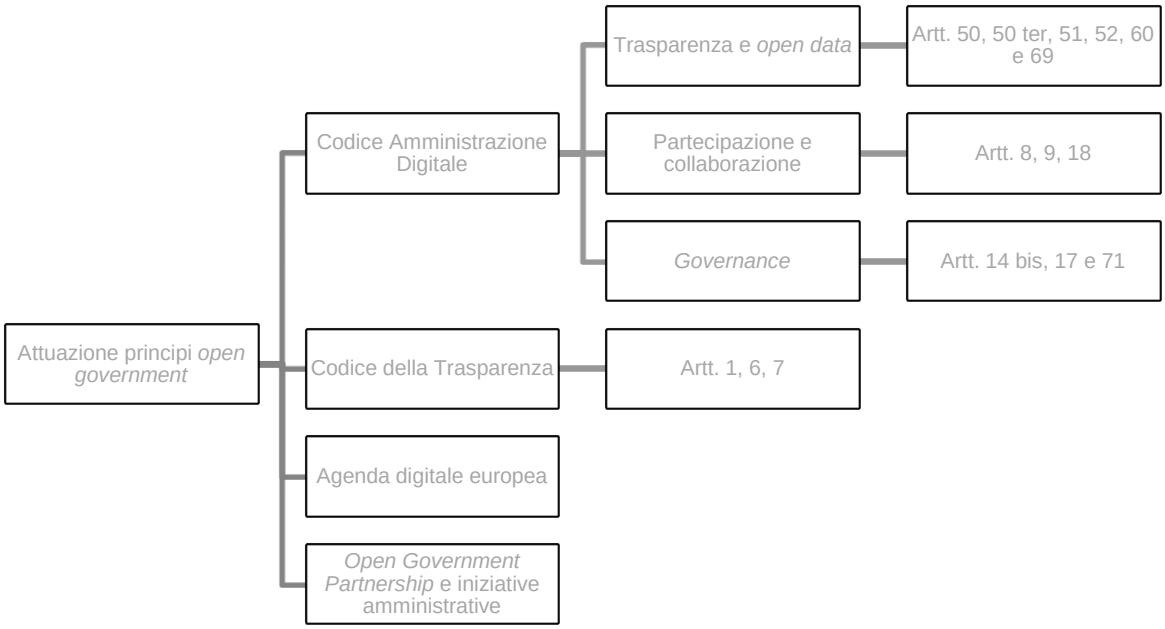
Un esempio significativo di *open government* è dato dalla piattaforma **Opencantieri**, un progetto promosso e gestito dal Ministero delle Infrastrutture e dei Trasporti (MIT) che presenta **informazioni complete e aggiornate sul processo di realizzazione delle infrastrutture pubbliche**. I dati prodotti ed esposti da fonti pubbliche sono integrati in un'unica piattaforma con sintesi e viste specifiche e le informazioni sono integralmente accessibili e scaricabili attraverso la pagina degli *open data* del MIT. Si tratta di un osservatorio sui lavori in corso che permette di conoscere a punto di realizzazione è un'opera pubblica, per quale importo è stata finanziata, quanto sta effettivamente costando, se e perché ritarda, quanti giorni di lavoro vi sono stati effettivamente dedicati. L'obiettivo primario è quello di promuovere la disponibilità dei dati relativi alla gestione finanziaria ed alla realizzazione delle opere pubbliche, stimolando la partecipazione dei cittadini, sviluppando attraverso la sperimentazione di modelli di gestione fondati sulla collaborazione in rete e sulla interazione tra cittadini e istituzioni. I dati esposti sono integrati dai diversi produttori, mentre la piattaforma si limita a tradurre i dati in alcuni indicatori essenziali per comprendere la

dislocazione, l'avanzamento dei lavori ed i costi delle infrastrutture strategiche per il paese.

Di rilievo nella promozione dell'amministrazione aperta è **Italiasicura,** cioè la **struttura di missione del Governo contro il dissesto idrogeologico e per lo sviluppo delle infrastrutture idriche**. Quasi contemporaneamente alla creazione della Struttura è stata lanciata una piattaforma web contenente informazioni e dati relativi a frane, alluvioni, emergenze, cantieri, progetti e interventi per la riqualificazione dell'edilizia scolastica; le informazioni sono in *open data* e integrate con i social network. Gli interventi relativi alla struttura sono specificati nelle tre sezioni (dissesto, acque pulite e scuole), accedendo alle quali è possibile avere informazioni sugli interventi specifici in atto in una certa zona del Paese, sugli interventi di edilizia scolastica, sul rischio di dissesto idrogeologico oppure sugli interventi pubblici sulle acque. In ogni sezione è presente una mappa interattiva che restituisce una cartografia interrogabile con i dati relativi alla sezione da cui è effettuato l'accesso, oltre ad una breve descrizione del contenuto; è possibile poi, visualizzare i dati ed effettuare il *download* degli stessi in modalità *open*.

L'obiettivo dell'azione è rendere maggiormente percepibile il problema della cura del territorio (sia per quanto riguarda la situazione del dissesto, sia per quanto riguarda la contaminazione delle acque) puntando sulla partecipazione dei cittadini e sulla loro consapevolezza. Alla base dello sviluppo della piattaforma vi è l'idea che i dati non debbano semplicemente essere resi pubblici, ma contestualizzati, semplificati e spiegati ai cittadini in una visione più complessiva di politiche di riduzione dei rischi, aiutando a comprendere e seguire le attività di prevenzione strutturale e di protezione civile decise sui territori, fornendo anche un attivo contributo nella mitigazione dei rischi.

L'ultima sezione del portale è quella relativa alle politiche di edilizia scolastica, che ha l'obiettivo di informare sulle attività del Governo per le ristrutturazioni e la messa in sicurezza delle scuole del Paese. Il portale è stato creato allo scopo di permettere ai cittadini di monitorare la realizzazione delle opere previste grazie allo sblocco dei fondi derivanti dall'allentamento del patto di stabilità (DPCM del 13, 30 giugno e del 28 ottobre, riepilogati nel DPCM del 24.12.2014) e si articola in sottosezioni che mostrano i finanziamenti volti a sostenere le nuove edificazioni di istituti scolastici e la ristrutturazione completa di quelli esistenti. Sono indicati gli interventi di messa in sicurezza delle scuole, di manutenzione straordinaria, per l'adeguamento alla normativa antisismica e per l'eliminazione delle barriere architettoniche, nonché per la rimozione dell'amianto.

Per quanto concerne le azioni concernenti il tema dell*'open data*, della promozione dell'innovazione sociale e dell'*e-government*, un'importante iniziativa è **OpenCoesione**, promossa dal Dipartimento per lo Sviluppo e la Coesione Economica del Ministero dello Sviluppo Economico, in collaborazione con diversi enti regionali e centrali. Il progetto ha rappresentato una

buona pratica in termini di trasparenza ed *accountability* delle **politiche di coesione**, sia in Europa che in Italia. L'iniziativa si rivolge a vari portatori di interessi, come cittadini singoli e organizzati, amministratori, tecnici e imprenditori dell'innovazione, ricercatori e giornalisti perché abbiano a disposizione **dati e informazioni per valutare l'efficacia e la coerenza dell'impiego delle risorse delle politiche di coesione**. Attraverso il portale OpenCoesione, infatti, è possibile verificare quali progetti si finanziano con i fondi europei, seguire il loro avanzamento ed anche sollecitare i processi di programmazione e attuazione attraverso iniziative di partecipazione e riuso.