Corso di formazione
Responsabile per la Transizione al Digitale

Modulo V

Il rapporto tra la transizione al Digitale e Privacy

A cura di

Avv. Michele Iaselli

M.5.1 L’e-government

La digitalizzazione dei servizi nel campo della pubblica amministrazione rimane uno degli argomenti più complessi e di difficile realizzazione sia per il proliferare di norme che spesso hanno disciplinato la materia in modo confusionario e non sempre attento sia per le concrete problematiche di carattere organizzativo e tecnologico.

Una tappa fondamentale è stata sicuramente il piano di e-government varato nel giugno 2000 dal Consiglio dei Ministri su iniziativa del Ministro della Funzione Pubblica, Franco Bassanini contraddistinto da una 1^ ed una 2^ fase. Tale progetto aveva come suo obiettivo fondamentale proprio quello di garantire ai cittadini l'accesso on-line a tutti i servizi erogati dalle pubbliche amministrazioni nell'ottica di quella che rappresentava la nuova frontiera di Internet.

Protagoniste dell'innovazione dovevano essere le amministrazioni locali, che nel modello decentrato e federale dello Stato rappresentavano il *front-office* dell'intero sistema amministrativo a disposizione diretta dei cittadini, mentre le amministrazioni centrali dovevano svolgere per lo più il ruolo di *back-office*.

L'idea di fondo era quella della realizzazione di un grande processo di innovazione tecnologica che coinvolgesse tutto il sistema pubblico italiano mettendolo così sullo stesso piano rispetto a quello di altri paesi più progrediti nelle nuove tecnologie della comunicazione.

Ma già allora ci si rese conto che per realizzare un simile processo c'era bisogno di una serie di condizioni che rendessero possibile l'integrazione fra le diverse attività e funzioni delle varie pubbliche amministrazioni e la loro fruibilità da parte dei cittadini.

La seconda fase di attuazione dell'e-government ha avuto come obiettivo principale l'allargamento alla maggior parte delle amministrazioni locali dei processi di innovazione già avviati, sia per ciò che riguarda la realizzazione dei servizi per cittadini e imprese, sia per ciò che riguarda la realizzazione di servizi infrastrutturali in tutti i territori regionali.

Purtroppo, come è noto, il progetto di e-government, per quanto ambizioso, non è riuscito a raggiungere gli obiettivi voluti per forti resistenze innanzitutto di carattere mentale oltre che per obiettive carenze infrastrutturali e professionali.

M5.2 L’agenda digitale

Sicuramente il lento ma inesorabile percorso del nostro paese verso la completa digitalizzazione di tutte le fondamentali attività di rilevanza pubblicistica ha conosciuto con l'Agenda digitale, i cui principi informatori sono contenuti nel Decreto-legge 18 ottobre 2012, n. 179 convertito dalla legge di conversione 17 dicembre 2012, n. 221, un momento importante e nello stesso tempo molto delicato poiché il nostro paese si dota di uno strumento normativo che, si spera, costituirà un’efficace leva per la crescita economica ed occupazionale.

Come noto i "pilastri" dell'Agenda Digitale europea sono:

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

Le misure dell'Agenda Digitale Italiana

- Documento digitale unificato
- Anagrafe nazionale e censimento della popolazione
- Pec e domicilio digitale
- Comunicazioni telematiche
- Biglietto elettronico e trasporto intelligente
- Open data
- Scuola digitale
- Sanità digitale
- Banda larga e digital divide
- Pagamenti elettronici
- Giustizia digitale
- Comunità intelligenti

M5.3 Aspetti di maggior impatto privacy nel codice dell'Amministrazione digitale (Spid, Open data. Documento informatico, PEC e gestione elettronica documentale)

Come è noto tutte le norme - emanate per favorire la diffusione delle nuove tecnologie e l'ammodernamento delle strutture pubbliche – sono state raccolte in un codice approvato con *il decreto legislativo del 7 marzo 2005, n. 82 recante il "Codice dell'Amministrazione Digitale" (CAD).*

Quest'ultimo decreto legislativo ha subito diverse modifiche ed integrazioni: D. Lgs. 4 aprile 2006, n. 159, dalla legge 24 dicembre 2007, n. 244, dalla legge 28 gennaio 2009 n. 2, dalla legge 18 giugno 2009, n. 69, dalla legge 3 agosto 2009, dal d.lgs. 30 dicembre 2010, n. 235, dalla legge n. 221/2012 (recante i principi dell'Agenda Digitale), dalla legge n. 98/2013 (decreto del fare), dal d.lgs. n. 179 del 26 agosto 2016 ed infine dal d.lgs n. 217 del 13 dicembre 2017.

Con le ultime riforme non solo si è proceduto ad una modifica ed integrazione delle norme del CAD ma ne sono state abrogate diverse anche attraverso vari accorpamenti e semplificazioni.
L'obiettivo è innanzitutto quello di promuovere e rendere effettivi i diritti di cittadinanza digitale dei cittadini e delle imprese, garantendo, contestualmente, il diritto di accesso ai dati, ai documenti e ai servizi di loro interesse in modalità digitale, semplificando le modalità di accesso ai servizi alla persona e realizzando - come indicato dal titolo con cui è rubricato l'art. 1 della legge n. 124 del 2015 - una vera e propria "*carta della cittadinanza digitale*".

Altro obiettivo fondamentale è quello di spostare l'attenzione dal processo di digitalizzazione ai diritti digitali di cittadini e imprese. Con la "carta della cittadinanza digitale" si riconoscono direttamente diritti a cittadini e imprese e si costituisce la base giuridica per implementare Italia Login, la piattaforma di accesso che, attraverso il Sistema pubblico d'identità digitale (SPID) e l'Anagrafe nazionale della popolazione residente, permetterà ai cittadini di accedere ai servizi pubblici - e a quelli degli operatori privati che aderiranno - con un unico nome utente e un'unica *password* (prenotazioni di visite mediche, iscrizioni a scuola, pagamento dei tributi).

Il sistema SPID assume sempre di più un ruolo centrale in questo nuovo CAD e viene definito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con specifico decreto ministeriale, identificano cittadini, imprese e pubbliche amministrazioni per consentire loro l’accesso ai servizi in rete.

Lo SPID, quindi, è un insieme di credenziali per accedere in rete a tutti i servizi della pubblica amministrazione e a quelli degli operatori commerciali che vi aderiranno. Lo SPID consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati per permettere ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

Con l'istituzione dello SPID le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi che alla fine avranno in tal senso una funzione solo residuale. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.

E’ chiaro, quindi, l’intento del legislatore di semplificare al massimo l’accesso ai servizi on line dei cittadini, superando le difficoltà connesse alle carte elettroniche, ma il pericolo “sicurezza” incombe sempre, poiché è evidente che con tale sistema si moltiplicano le identità digitali di un cittadino, che saranno diverse per ogni servizio e la prospettiva lascia perplessi. E’ anche vero che il sistema è continuamente monitorato dall’Autorità Garante giustamente preoccupata, ma è anche vero che se una singola identità digitale crea problemi figuriamoci tante.

L'opportunità delle ultime riforme dell'intero CAD nasce anche dalla necessità di adeguare lo stesso al Regolamento comunitario n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari nel mercato interno pubblicato nella G.U. dell'Unione Europea del 28 agosto 2014 che è entrato in vigore nel nostro ordinamento il 1 luglio 2016.

Il Regolamento è noto con l'acronimo e-IDAS che sta per electronic IDentification Authentication and Signature (eTS electronic Trust Services) e stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche.

Il Regolamento, quindi, innanzitutto disciplina l'identificazione elettronica intesa come "*il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica*", preoccupandosi del riconoscimento reciproco fra gli Stati membri dei mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro.

L'identificazione elettronica va distinta dalla c.d. "autenticazione" intesa come "*un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica*".

Il responsabile per la transizione al digitale

La figura del responsabile della transizione digitale rimane ancora una figura poco chiara nell'ambito della pubblica amministrazione che non va confusa con quella del difensore civico digitale disciplinata dalla stessa norma (art. 17, comma 1-quater, del CAD) ma prerogativa ormai dell'Agenzia per l'Italia Digitale (AgID) che a seguito di quanto previsto dalla più recente riforma del 2017 ha organizzato uno specifico ufficio per tale esigenza.

In effetti il responsabile della transizione digitale nasce con la riforma Madia (d.lgs. n. 179/2016) che con l'art. 15 riformulava l'art. 17 del CAD, prevedendo che "le pubbliche amministrazioni garantiscano l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'art. 71 del CAD, attraverso l'affidamento ad un unico ufficio dirigenziale generale della transizione alla modalità operativa digitale e dei processi di riorganizzazione finalizzati alla realizzazione di una amministrazione digitale aperta". In precedenza, difatti, si parlava sempre di un unico ufficio dirigenziale generale, ma responsabile solo del coordinamento funzionale.

Con l'avvento della più recente riforma del CAD (d.lgs. n. 217/2017) il relativo art. 17 oltre a sostituirne la rubrica, ha apportato modifiche di drafting al comma 1 dell'articolo 17 del decreto legislativo 7 marzo 2005, n. 82, prevedendo anche nuovi compiti di questa figura dirigenziale.

Gli open data

L’art. 7 del d.lgs. n. 33/2013 prevede i c.d. open data sancendo che i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell'accesso civico di cui all'articolo 5, sono pubblicati in formato di tipo aperto ai sensi dell'articolo 68 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità.

Per Open data si intendono i dati aperti, cioè informazioni che sono liberamente accessibili a chiunque. Fra i principi essenziali degli open data troviamo:

- *accessibilità*, intesa come disponibilità nel potervi entrare, cioè poter leggere il dato senza particolari difficoltà;
- *disponibilità*, cioè assenza di restrizioni, limitazioni di alcun genere (brevettuali o di diritto d'autore) alla loro accessibilità;
- *replicabilità*, nel senso che questi dati devono poter essere facilmente riproducibili e riutilizzabili, permettendo all'utente che li voglia utilizzare di poterne leggere e riprodurre il contenuto;
- *trasparenza*, poter leggere un dato senza doversi munire di specifici strumenti tecnici o interpretativi per avvicinarsi al contenuto dei dati;
- *intelligibilità*, cioè dati comprensibili senza dover utilizzare particolari conoscenze a riguardo;
- *non discriminazione*, tutti devono essere in grado di usare, riutilizzare e ridistribuire i dati;
- *neutralità tecnologica*, nel senso che bisogna evitare di imporre vincoli tecnologici ed economici agli utenti.

Viene, quindi, raccomandato, dalle linee guida per i siti web delle pubbliche amministrazioni l'uso dei seguenti formati aperti e standardizzati: Html/Xhtml per la pubblicazione di informazioni pubbliche su Internet; Pdf con marcatura (standard Iso/Iec 32000-1:2008); Xml per la realizzazione di database di pubblico accesso ai dati; Odf e Ooxml per documenti di testo; Png per le immagini; Ogg per i file audio; Theora per i file video; Epub per i libri elettronici.

Ovviamente quando si parla di open data il passaggio alla trasparenza amministrativa è immediato e l'art. 7-bis del d.lgs n. 33/2013 nel disciplinare il riutilizzo dei dati pubblicati regola necessariamente i rapporti con la normativa in materia di protezione dei dati personali chiarendo che gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, comportano la possibilità di una diffusione dei dati medesimi 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 ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.

Si precisa, inoltre, che la pubblicazione nei siti istituzionali di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali sebbene la Corte Costituzionale con sentenza 23 gennaio - 21 febbraio 2019, n. 20 abbia dichiarato l'illegittimità costituzionale della disposizione dell'art. 14, comma 1-bis, del d.lgs. n. 14 marzo 2013, n. 33 nella parte in cui prevede che le pubbliche amministrazioni pubblicano i dati di cui all'art. 14, comma 1, lettera f), dello stesso decreto legislativo anche per tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione.

La norma ancora prevede che nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

Sono inevitabili, quindi, in materia gli impatti con la normativa posta a tutela dei dati personali e la stessa Autorità Garante ha più volte specificato che se priva di adeguati criteri discretivi, la divulgazione di un patrimonio informativo immenso e sempre crescente (quale quello delle pubbliche amministrazioni) rischia di mettere in piazza spaccati di vita individuale la cui conoscenza è inutile ai fini del controllo sull'esercizio del potere ma, per l'interessato, può essere estremamente dannosa.

Con l'adozione di apposite Linee guida (provvedimento del 15 maggio 2014), il Garante è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.
Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.

Prima di procedere alla pubblicazione sul proprio sito web la P.A. deve:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari, come ricordato al punto precedente.

Un eccesso indiscriminato di pubblicità rischia, peraltro, di occultare informazioni realmente significative con altre del tutto inutili, così ostacolando, anziché agevolare, il controllo diffuso sull'esercizio del potere e degenerando in una forma di sorveglianza massiva.

Per la trasparenza c'è bisogno di un approccio qualitativo e non meramente quantitativo: **meno dati ma più qualificati**.

In effetti, secondo l'Autorità Garante, l'attuale disciplina sulla trasparenza andrebbe rimodulata, prevedendo che ove l'accesso coinvolga dati personali di terzi, esso possa essere effettuato solo previo accertamento della prevalenza dell'interesse perseguito dall'accesso ovvero, previo oscuramento dei dati personali presenti.
Tale previsione andrebbe poi completata con un generale divieto di comunicazione di dati sensibili o giudiziari nonché di dati personali di minorenni, in osservanza della tutela rafforzata accordata dall'ordinamento interno e dal diritto dell'Unione europea a tali categorie di dati personali.

Il documento informatico

Il documento informatico è definito dal CAD come «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

Il valore giuridico e probatorio di un documento informatico è sicuramente collegato al tipo di firma elettronica che lo contraddistingue.

Allo stato attuale il Codice dell'Amministrazione digitale distingue tra quattro tipologie di firma e cioè:

Firma elettronica pura e semplice

Essa è definita dal CAD come l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica avanzata

Firma elettronica avanzata:

- una firma elettronica che è connessa unicamente al firmatario;

- che è idonea a identificare il firmatario;

- che 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;

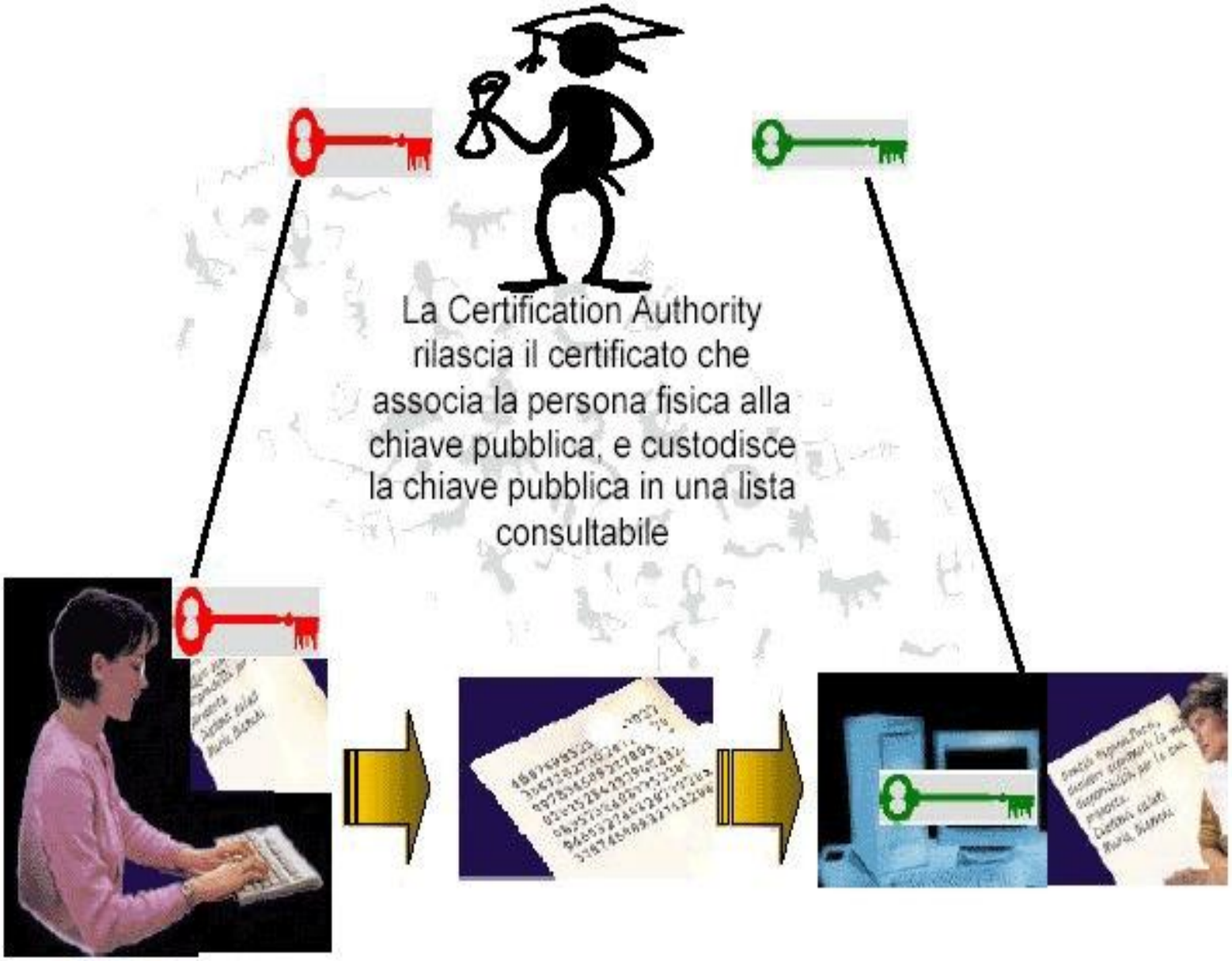
- che è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati (artt. 3 e 26 del regolamento e-IDAS).

Firma elettronica qualificata

Si tratta di 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 (art. 3 del Regolamento e-IDAS).

Firma digitale

E’ 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.



La Certification Authority rilascia il certificato che associa la persona fisica alla chiave pubblica, e custodisce la chiave pubblica in una lista consultabile

Il mittente firma con la sua chiave privata un documento

Il messaggio firmato, insieme al certificato del mittente rilasciato dalla CA, raggiunge il destinatario

Il destinatario, usando la chiave pubblica del mittente, riesce a determinare l'autenticità dello stesso e l'integrità del messaggio

Alla luce delle ultime riforme l'intenzione è quella di garantire maggiore certezza giuridica in materia di formazione, gestione e conservazione dei documenti digitali prevedendo che non solo quelli firmati digitalmente - o con altra firma elettronica qualificata - ma anche quelli firmati con firme elettroniche diverse, al ricorrere di specifiche condizioni identificate dall'AgiD, possano produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza che debba essere un giudice, caso per caso, a valutare al riguardo.

In particolare, il nuovo art. 20 del CAD - modificando la previgente disciplina che demandava esclusivamente agli organi giudicanti la possibilità di valutare liberamente in giudizio l'idoneità dei documenti informatici a fini probatori - prevede che il documento informatico soddisfi il requisito della forma scritta e abbia l'efficacia di cui all'art. 2702 c.c. qualora sia sottoscritto con una firma digitale, qualificata o avanzata, o, nel caso di documenti sottoscritti con firme elettroniche differenti, qualora rispetti gli standard tecnici individuati dall'AgID con specifiche linee guida, mentre, nei restanti casi, il valore probatorio del documento informatico è rimesso al libero giudizio degli organi giudicanti.

La gestione elettronica documentale

Lo sviluppo di strumenti quali la firma elettronica ed il protocollo informatico uniti all'espansione dell'uso della posta elettronica, rende possibile la realizzazione di una gestione completamente automatizzata dei flussi documentali e la conseguente attuazione di profonde innovazioni nelle modalità di lavoro delle unità organizzative.

La gestione documentale consiste in realtà in una macro-categoria, che comprende attività assai eterogenee, che variano a seconda del grado di funzionalità che si desideri attuare, ma che trovano una logica ben precisa per il loro accorpamento: ovvero il loro comune presupposto fondamentale, che è quello della dematerializzazione dei documenti cartacei e quindi della disponibilità degli stessi a livello informatico.

Le fasi del documento informatico

FORMAZIONE
(originale informatico, copia per immagine, copia informatica, duplicato)

Integrità, immodificabilità, autenticità

Le Regole Tecniche

GESTIONE DOCUMENTALE
(protocollo - registrazione e segnatura di protocollo, classificazione, organizzazione e fascicolazione, assegnazione, reperimento)

Contestualizzazione, archiviazione, ricercabilità

CONSERVAZIONE
(verifica, consolidamento, mantenimento leggibilità nel tempo, sicurezza)

Appare, quindi, chiaro che la vera dematerializzazione in realtà non può ridursi ai processi di digitalizzazione dei documenti, bensì consiste nel faticoso e complesso intervento di semplificazione dei processi e di diminuzione delle fasi e dei passaggi del processo decisionale, come del resto indicato negli obiettivi della legge 241 del 1990 da ormai 20 anni.

Bisogna, però, chiarire che la dematerializzazione o meglio il processo di informatizzazione della memoria documentaria, deve includere inoltre, per produrre risultati di qualche efficacia, il controllo sulla corretta formazione del documento e il governo del ciclo del documento in tutte le sue fasi incluso quello della conservazione: nessun processo di trasformazione può avere successo se non prevede la definizione di procedure e il controllo gestionale pianificato di tutte le fasi.

Riguardo la conservazione sostitutiva dei documenti informatici, l'art. 43 del CAD sancisce 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.

In sintesi il sistema di conservazione dei documenti informatici deve assicurare, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida.

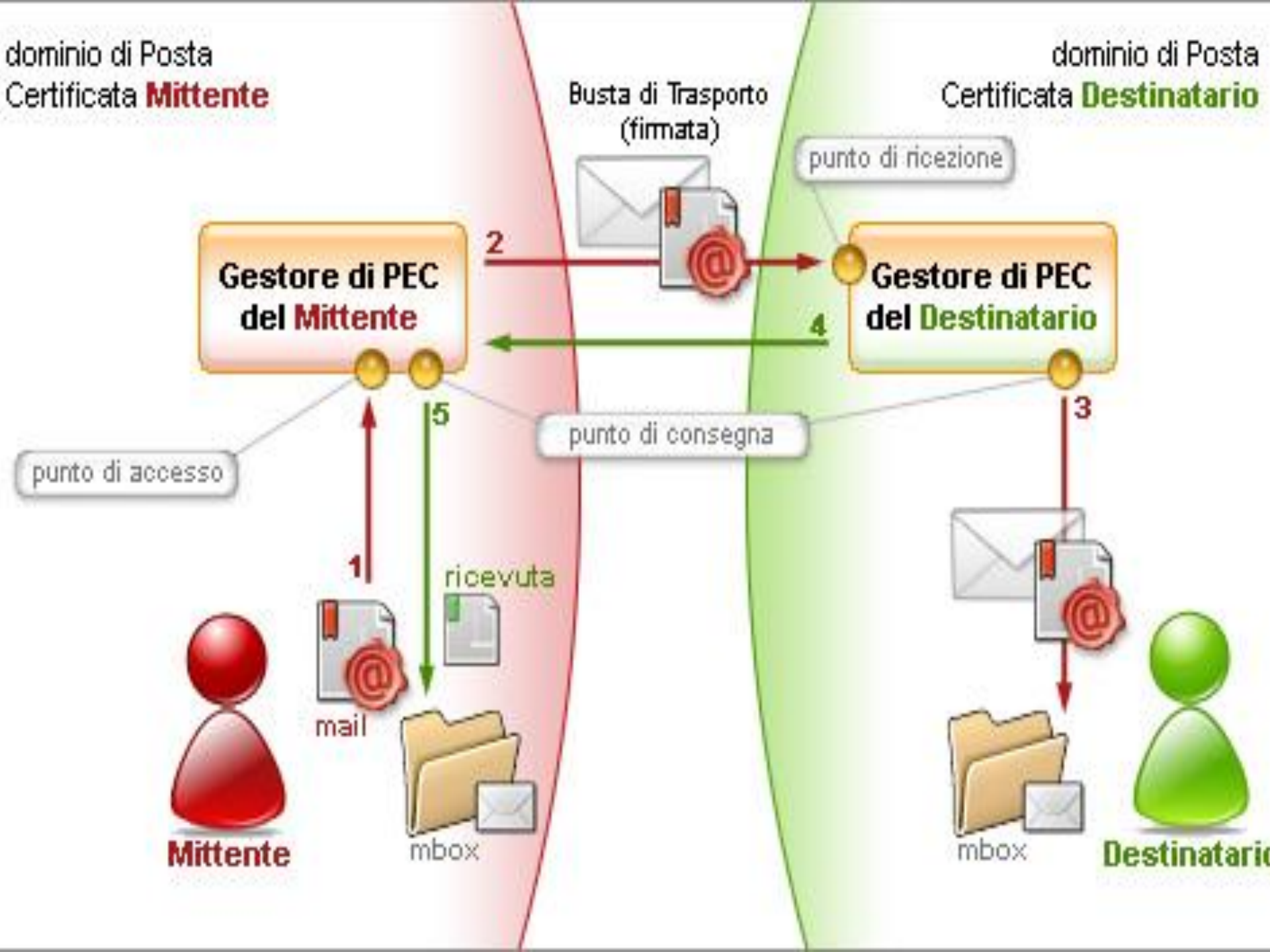
Al comma 1-bis dell'art. 44 del CAD si introduce la figura del responsabile della gestione dei documenti informatici che deve operare d'intesa con il responsabile della transizione al digitale, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196 (ora superato), ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza.

Al comma 1-quater dell'art. 44 del CAD si prevede la possibilità per il responsabile della conservazione, che opera a sua volta d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, di chiedere la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.

La posta elettronica certificata

Il Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) fa esplicito riferimento alla posta elettronica certificata all'art. 48 con rinvio al D.P.R. 68/2005 per la disciplina specifica, anche se il Consiglio di Stato avrebbe gradito (v. parere n° 11995 dell'Adunanza del 7.2. 2005) l'assorbimento dell'intero Decreto nell'ambito del CAD così come è avvenuto con il Sistema Pubblico di Connettività.

"Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici – significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale.


dominio di Posta Certificata Mittente
Busta di Trasporto (firmata)
dominio di Posta Certificata Destinatario
punto di ricezione
Gestore di PEC del Mittente
2
Gestore di PEC del Destinatario
4
5
punto di consegna
3
punto di accesso
1
ricevuta
mail
mbox
mbox
Mittente
Destinatario

M5.4 L’e-government 4.0

Come si è avuto modo di sottolineare il lungo ed ancora non perfezionato percorso verso l'amministrazione digitale è stato contraddistinto da diverse fasi: il piano nazionale di e-government risalente al 2000, il Codice dell'Amministrazione Digitale, l'Agenda Digitale. Oggi possiamo affermare che stiamo attraverso una fase 4.0 verso la digitalizzazione della PA contraddistinta da un progresso tecnologico sempre più avanzato e che ha necessità di essere regolamentato con riferimento ad aspetti etici, giuridici e principalmente di protezione dei dati personali.

Si tratta di una vera sfida che vede spesso contrasti apparentemente indissolubili ma che possono essere risolti proprio nell'ottica di quei principi ispiratori del GDPR com le privacy by design, la trasparenza e l'accountability.

Cercheremo di analizzare le principali implicazioni e problematiche sorte a seguito dell'avvento dell'intelligenza artificiale, dei big data ed IoT e della blockchain.

M5.5 L’intelligenza artificiale

Negli ultimi tempi, in diversi settori, sta assumendo una grande rilevanza il contributo dell'intelligenza artificiale intesa come ricerca per tentare di simulare ed emulare attraverso i computer alcuni dei comportamenti ritenuti caratteristici dell'intelletto umano.

Gli obiettivi dell'intelligenza artificiale sono essenzialmente due:

- approfondire e comprendere i principi che rendono possibile l'intelligenza (il computer viene usato per simulare le teorie sull'intelligenza);
- progettare computer dotati di capacità simili a quelle umane senza, però, tentare di imitare esattamente i processi informativi degli esseri umani.

I due approcci sono, naturalmente, correlati in quanto il risultato delle ricerche su come la gente risolve i problemi può spesso dare notevoli contributi per le tecniche di *problem-solving* attraverso l'uso dei computer.

L'intelligenza artificiale, quindi, comprende, da un lato, la c.d. *scienza cognitiva*, che studia l'intelligenza al fine di rappresentarla in modelli che possano essere trasferiti in applicazioni informatiche, d'altro lato, *l'intelligenza artificiale in senso stretto*, che si occupa delle tecnologie per tali applicazioni.
Quest'ultima, a sua volta, è stata divisa in *intelligenza artificiale forte*, intesa a duplicare la mente negli elaboratori, cioè a creare computer in grado di comprendere e di possedere stati cognitivi, ed in *intelligenza artificiale debole* intesa a realizzare sistemi informatici capaci di prestazioni normalmente attribuite all'intelligenza umana, pur senza assumere alcuna analogia tra le menti e i sistemi informatici.

Nel 1956, alla conferenza di Dartmouth, il workshop in cui viene utilizzata per la prima volta la terminologia “intelligenza artificiale”, vengono mostrati due programmi che segnano un'altra importante tappa dello sviluppo dell'IA. I programmi, che furono sviluppati dagli studiosi Allen Newell, J. Clifford Shaw e Herb Simon, erano i cosiddetti "Logic Theory Machine" e "General Problem Solver" (GPS).
In realtà la conferenza si segnala per una svolta epocale nel campo dell’IA.

Cognitivismo = sistemi esperti

Connessionismo = Reti neurali

L'art. 22 del GDPR nel disciplinare la cd. profilazione automatica fa indubbiamente riferimento a programmi e tecniche di IA che oggi sono particolarmente all'avanguardia e che tra l'altro sono particolarmente utili anche nel campo dei big data.

M5.6 I big data

Il termine **big data** ("grandi masse di dati" in inglese), o **megadati**, indica genericamente una raccolta di dati così estesa in termini di *volume*, *velocità* e *varietà* da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza. Il termine è utilizzato in riferimento alla capacità (propria della scienza dei dati) di analizzare ovvero estrapolare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati, allo scopo di scoprire i legami tra fenomeni diversi (ad esempio correlazioni) e prevedere quelli futuri. La disciplina può essere vista come un'evoluzione dei tradizionali metodi di business intelligence, allargata a moli di dati ancor più variegate e soprattutto più voluminose.

L'avvento del web 2.0 inteso come evoluzione della rete e dei siti internet caratterizzata da una maggiore interattività che pone l'utente al centro della rete ha comportato la possibilità di avere a disposizione una grande mole di informazioni che possono essere utili per diverse finalità: profilazione, ricerche scientifiche, statistiche, ecc.

Ma anche ulteriori forme di evoluzione della Rete consentono di acquisire notevoli informazioni specialmente con riferimento ai gusti ed alle abitudini degli individui, si pensi all'Internet of Things (IoT).

Con il termine Internet of Things (IoT) si fa riferimento ad infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es. RFID, bluetooth etc.), sia tramite una rete di comunicazione elettronica.

Nel caso dei big data il contributo dell'intelligenza artificiale si colloca nella cd. estrazione di conoscenza che è una tecnica che consente di filtrare, navigando nella rete, solo le informazioni pertinenti ad un dato settore di interesse (ad esempio solo le informazioni finanziarie); gli strumenti si basano su due tipici paradigmi di I.A.: i nuclei concettuali (conceptual cluster) ed i parser del linguaggio naturale.

Con i primi vengono descritti gli elementi della materia di interesse mediante tutte le possibili espressioni e forme linguistiche (ad es. società, capitali, azioni, stock, interesse, ratei, profitto, ecc.), segnalando anche quali caratteristiche ci si aspetta dai dati che si cercano, ad esempio, in notizie di carattere finanziario ricorreranno i nomi di società quotate in borsa, di organismi finanziari, di quote azionarie, ecc. Con il secondo strumento si filtrano (parsing) le stringhe di parole in modo da rintracciare all'interno le 'parole civetta'.

Una tecnica più raffinata di I.A. da applicare sempre in tale settore è il data mining. Letteralmente mining è l'attività del minatore, cioè lo scavo, l'estrazione di materiali preziosi da materiali di scarto: nel data mining il materiale prezioso da rintracciare è la conoscenza, cioè informazioni nuove e originali su determinati fenomeni, estratte da grandi quantità di dati. La conoscenza scoperta con il data mining è qualcosa di più del risultato di analisi statistiche, in quanto dovrebbe evidenziare non solo la frequenza di certi fenomeni, ma i modi in cui vengono a concatenarsi circostanze o fattori (association rules).

Con riferimento all'identità digitale si parla di *digital footprint,* termine che viene comunemente utilizzato per indicare le tracce di dati che vengono disperse nella rete a seguito di determinate interazioni avvenute all'interno dell'ambiente digitale, questi dati contengono usualmente informazioni riguardanti le diverse interazioni che un soggetto può eseguire in un contesto digitale. Questi dati ed informazioni possono concorrere nel formare un' identità digitale.

A tal fine è possibile individuare almeno due tipi di informazioni che possono essere reperite on-line e riguardanti un soggetto determinato, un primo tipo, che potremmo definire di informazioni primarie e riguardanti i caratteri personalissimi dell'individuo, ed altri tipi di informazioni secondarie, riguardanti le abitudini sociali ed i gusti commerciali dell'utente interessato, questi due tipi di informazioni, elaborate tra loro, formano il cd. profilo-utente.

Come noto, la maggior parte dei moderni dispositivi di comunicazione, al momento del loro utilizzo attraverso il collegamento ad internet, frammentano e disperdono delle tracce che provano l'utilizzo del dispositivo e la contestuale presenza dell'utente in rete.
Nella pratica il problema della profilazione e della dispersione dei dati personali, si manifesta in modo particolare nei momenti della navigazione in internet mediante browser (si pensi ai cookies) e nell'utilizzo delle più comuni piattaforme di social networking come strumenti relazionali e di comunicazione.

A tal fine vengono sempre più utilizzate anche tecniche di reperimento di informazioni utili al ciclo di intelligence tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i Social Media come la SOCial Media INTelligence (SOCMINT).

L'obiettivo principale della profilazione è la pubblicità comportamentale, che pensata e cresciuta nel mondo delle comunicazioni informatiche, prevede il tracciamento delle informazioni rilasciate dagli utenti durante la navigazione in internet, al fine di creare segmenti pubblicitari *ad personam,* modellati sugli interessi dell'utente considerato.

M5.7 La blockchain

La novità di maggior rilievo dal punto di vista giuridico-tecnologico della recente conversione in legge n. 12/2019, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione è sicuramente rappresentata dall'art. 8-ter dove vengono definite le tecnologie basate sui registri distribuiti e gli smart contract.

Per smart contract si intende "un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse". Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

Indubbiamente è encomiabile il tentativo del legislatore di definire queste nuove tecnologie fortemente incentivate dalla stessa commissione europea, basti vedere alla Risoluzione del Parlamento europeo del 3 ottobre 2018 o anche al Libro bianco "Raccomandazioni per adottare standard comuni in Europa sulla Blockchain e sui registri distribuiti (distributed ledger)", a cura del Comitato europeo per la standardizzazione (Cen) e del Comitato europeo per la standardizzazione elettronica (Cenelec) che affronta la delicata problematica dei requisiti che dovranno avere i servizi basati sulle nuove tecnologie blockchain per abilitare servizi sicuri e di qualità.

La blockchain sostanzialmente è:

- Una «catena di blocchi» che crea un registro digitale. Le operazioni, come un atto di compravendita o transazioni in moneta virtuale, vengo vagliate da molteplici operatori che ne garantiscono l'autenticità.
- Un database (registro) distribuito per la gestione di transazioni crittografate ed è aperta a tutti.
- Il database è composto da una serie di blocchi che archiviano un insieme di transazioni validate dai nodi della catena.
- La catena è composta da nodi, transazioni, blocchi, ledger/registri, funzioni di hash.
- Le transazioni, verificata la loro correttezza, vengono archiviate su tutti i nodi della blockchain.

La grande sicurezza, trasparenza e versatilità dello strumento sta vincendo le iniziali resistenze di molti operatori ed ormai sono diversi i campi di utilizzazione della blockchain.

Rimangono alcune perplessità sull'eccessiva rapidità ed anche approssimazione del legislatore nel definire tali fenomeni estremamente complessi dal punto di vista tecnico.

In determinati casi un divario temporale tra l'emergere di una tecnologia e la sua successiva regolamentazione non può essere valutato in termini completamente negativi poiché consente di avere più tempo per valutare le possibili conseguenze e prendere così decisioni politiche più corrette e consapevoli.

E’ necessario, difatti, anche prevedendo rischi futuri di attività che sono in continua evoluzione, predeterminare un quadro etico e giuridico corretto che possa consentire l’adozione di regole appropriate, ed orientare i successivi processi di ricerca e di produzione con valori etici e legali riconosciuti a cui la progettazione di prodotti innovativi si debba conformare.

Per quanto riguarda i dati pubblici è necessario ed importante tutelare la loro natura pubblica. Contemporaneamente è altrettanto determinante salvaguardare la tutela della privacy, ovvero la natura confidenziale, delle informazioni trattate. Queste caratteristiche, tanto importanti quanto opposte, mal si conciliano con lo stato attuale dello sviluppo tecnologico degli Smart Contracts su Blockchain rendendone l'utilizzo, ad oggi, complesso e costoso.

D’altronde come sottolineato dal Parlamento Europeo nella stessa Risoluzione è opportuno che, per tali tecnologie di registro, si affrontino adeguatamente anche le problematiche attinenti proprio al settore della protezione dei dati personali dove il Regolamento europeo n. 2016/679 ha introdotto importanti principi come quello di accountability o il principio della privacy by design che diventa fondamentale con riferimento alla blockchain.

La presenza di dati personali all'interno di un sistema contraddistinto dalla tecnologia di registro può creare non pochi problemi in merito al rispetto dell'attuale normativa comunitaria poiché diventerebbe, innanzitutto, difficilmente gestibile la presenza di errori con riferimento agli stessi dati che rappresentano il logico presupposto di una "catena" davvero poco elastica per ragioni di sicurezza. Inoltre per le stesse ragioni, come è noto, poiché il dato personale non può essere conservato per sempre, l'eventuale cancellazione nel rispetto del GDPR diventerebbe non poco difficoltosa.

La predisposizione di un sistema contraddistinto da tale tecnologia implica, inevitabilmente, nell'ottica dei principi generali del GDPR sopra evidenziati, uno studio approfondito sui rischi, non di poco conto, connessi in materia di protezione dei dati personali per cui sarebbe necessario quanto meno condurre un'accorta valutazione di impatto sulla protezione dei dati personali alla luce dell'art. 35 del GDPR che tenga conto delle specifiche peculiarità dello strumento tecnologico.

In altri termini è giusto come sottolineato dalla Commissione europea studiare ed approfondire tali tecnologie ma non giungere a conclusioni troppo affrettate visto che il nostro paese ha già vissuto precedenti esperienze vedi la firma digitale o la posta elettronica certificata dove ha anticipato l'introduzione e la regolamentazione di tecnologie rimanendo però drammaticamente isolato per la mancata condivisione nell'ambito dell'Unione europea.