KnowIT

Rivista scientifica per i manager della governance digitale e della privacy

L'innovazione non va in vacanza

KnowIT. Periodico trimestrale. Anno II N. 2 - Luglio 2017 - ISSN 2532-1684

Indice

KnowIT. Rivista scientifica trimestrale gratuita per i manager della governance digitale e della privacy.

Anno 2 - Numero 2 - Luglio 2017 - Testata iscritta al n. 6/2016 del Registro della Stampa del Tribunale di Lecce il 23 maggio 2016 - ISSN 2532-1684

Direttore responsabile: Silvia Riezzo

Direttore editoriale: Andrea Lisi

Editore: Clio S.r.l. Via 95° Rgt. Fanteria n°70 - 73100 Lecce. Tel. +39 0832 344041 - Fax +39 0832 340228 - www.clio.it - info@clio.it

EDITORIALE: La “metamorfosi” del documento informatico

Andrea Lisi - *Direttore Editoriale KnowIT, Presidente ANORC Professioni*

“Un mattino, al risveglio da sogni inquieti, Gregor Samsa si trovò trasformato in un enorme insetto. Sdraiato nel letto sulla schiena dura come una corazza, bastava che alzasse un po’ la testa per vedersi il ventre convesso, bruniccio, spartito da solchi arcuati; in cima al ventre la coperta, sul punto di scivolare per terra, si reggeva a malapena. Davanti agli occhi gli si agitavano le gambe, molto più numerose di prima, ma di una sottigliezza desolante”. L’incipit del racconto *La metamorfosi* di Franz Kafka non può non farci ricordare il cambiamento radicale che sta vivendo oggi l’arte di documentare. Il documento informatico rischia effettivamente di avere molte più ramificazioni oblique e una sottigliezza giuridico/archivistica tale da rivelarsi desolante.

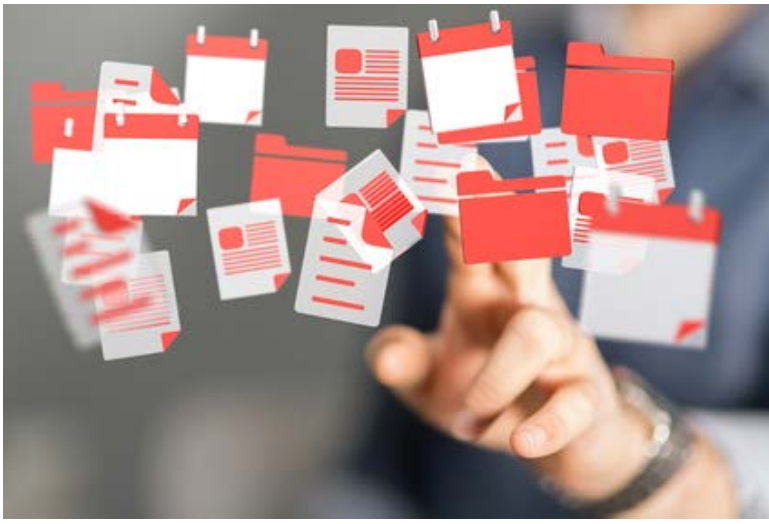
Più volte in questi anni mi sono soffermato ad approfondire il significato del cambiamento rivoluzionario insito nelle forme e nei modi di “documentare in digitale”. Proprio sulle pagine di questa Rivista con Francesca Cafiero abbiamo approfondito **il passaggio epocale dal segno (res signata), tipico della scrittura analogica, alle nuove forme per documentare con certezza (attraverso l’affidamento del processo a figure responsabili)**, peculiari di questi anni[1].

Nella frenesia del mondo informatico **ciò che si documenta sfugge sempre di più all’archivio**, sia in ambito strettamente giuridico o amministrativo, sia in altri ambiti come quello letterario, musicale o cinematografico, dove tutti i contenuti sono ormai digitali e spesso vengono condivisi in ambienti social, sottraendone la diffusione al controllo dei singoli autori. **Tutto viene partecipato, contaminato, diffuso nella miriade dei bit perdendo il senso del contesto e dell’affidabilità delle fonti di pubblicazione**.

Tutto è diffuso e disponibile ovunque, ma l’ovunque ubiquo è indeterminato e indeterminabile e **spesso** (e incredibilmente) **favorisce la dispersione del documento. Il dato** (forse) c’è ancora, ma nella sua dissennata contaminazione ha lasciato per strada la certezza giuridica e il contesto archivistico. E quindi **non è più garantito nella sua autenticità**.

Ovvio, allora, che vadano trovati nuovi metodi di documentare, che preservino la certezza giuridica e il contesto archivistico, in modo completamente nuovo, originale e seguendo le esigenze peculiari insite nei binari dell’innovazione digitale. Ad esempio, in una PA ormai “ciò che non è pubblicato sul sito web non esiste”[2], e quindi l’archivio deve partire dal portale istituzionale e da lì si devono sviluppare gli scenari della certezza giuridico-amministrativa, tutelando la pubblica fede tipica dell’archivio. E **allo stesso modo occorre guardare in modo approfondito ai contesti di e-commerce** nei quali l’esigenza è quella di documentare correttamente la trasparenza verso il consumatore o la trasparenza informativa richiesta dalla normativa privacy (e non è cosa ovvia). Anche il consenso viene acquisito in modo nuovo, attraverso metodologie che correlano identità verificate on line e successivi comportamenti giuridicamente rilevanti[3]. E tutte queste nuove modalità di sviluppare atti, fatti, manifestazioni di volontà vanno riportate a una nuova logica giuridico-archivistica (in un ambiente informatico che deve necessariamente rimanere *user friendly*).

Tutto cambia, si trasforma, assume nuovi connotati e, se pur astrattamente riconducibile - dal punto di vista giuridico - alle fattispecie della scrittura privata, o delle riproduzioni informatiche/fotografiche o anche alle intuizioni del legislatore del 1942, allorquando si regolamentava l’incredibile novità tecnologica del telegramma, non può non apparire lapalissiano **che lo sguardo dell’interprete (inevitabilmente multidisciplinare) deve guardare oltre, verso le tante** singole (e sterminate) **sfaccettature della rivoluzione digitale, sussumendole in fattispecie astratte** e provando così a reinterpretarle nel nuovo contesto **in modo indipendente** (se possibile) **dalla singola tecnologia** che è in continuo divenire.



“Nel caso degli archivi digitali l’evoluzione ha riguardato di volta in volta il sistema operativo, gli applicativi, i supporti di archiviazione, i dispositivi di scrittura. Preservare a lungo termine le memorie collettive e personali degli ultimi decenni è un’impresa resa particolarmente complessa dalla necessità di integrare competenze appartenenti ad ambiti considerevolmente diversi: discipline letterarie, tecniche archivistiche, tecnologia dell’informazione, questioni giuridiche, aspetti amministrativi. Inoltre, la gestione dell’archivio digitale presuppone l’aggiornamento costante dei modelli di dati, degli standard e delle procedure per far fronte alla crescente varietà delle fonti documentarie”[4].

Ma se da una parte è difficile documentare in un’epoca caratterizzata da una inevitabile “dedocumentalizzazione”[5], dall’altra non possiamo esimerci dal comprendere appieno cosa sia oggi la “forma scritta digitale”, riportandola alle sue radici storiche di *verba volant, scripta manent*.

Quindi oggi, anche secondo le nuove definizione di documento elettronico[6] e di documento informatico[7], **cosa può ritenersi forma digitale rilevante e affidabile? Cosa può ritenersi valido** dal punto di vista della forma scritta ***ad probationem* o *ad substantiam?* Cosa può definirsi scrittura privata dal punto di vista digitale?**

Non ci sono risposte ovvie a queste domande e nell'evoluzione costante (ed eccessiva) del Codice dell'amministrazione digitale purtroppo alla maggior parte degli interpreti il problema sfugge del tutto e alcune volte si raggiungono "certezze relative" basate su pronunce dalla giurisprudenza scostanti, mutevoli o poco motivate, come ad esempio la recente sentenza in cui si afferma che il messaggio WhatsApp garantisce la forma scritta ai fini del valido licenziamento del lavoratore[8]. Pronuncia tutta da verificare e commentare nella sua valenza ed esattezza ermeneutica (e sono certo che in futuro lo faremo lungo le pagine di questa Rivista).

Del resto, c'è davvero oggi differenza sostanziale tra un Registro IVA o un Libro Giornale che contengono i dati contabili aggiornati dell'impresa oppure un Registro di protocollo informatico di una PA o un Registro di Log di un portale di e-commerce dal quale si evincono i dati aggiornati e profilati sui gusti e le abitudini dei clienti on line[9]? Ormai si tratta sempre e solo di registrazioni indipendenti da supporti e sempre più leggibili in modo "mediato", rese disponibili e autentiche attraverso l'opera di intermediari responsabili. Ma **quando il documento informatico è in grado**, appunto, **di documentare con caratteristiche parificabili alla forma scritta analogica[10]?**

In fin dei conti, occorre ragionare proprio sulle moderne strade in cui si muove oggi la rappresentazione informatica assumendo la connotazione specifica di documentare azioni, fatti o manifestazioni di volontà ed elaborare delle decisioni importanti dal punto di vista ermeneutico per gli scenari futuri. **Decisioni che devono coinvolgere tutti gli interpreti (giuristi, informatici, archivisti, diplomatisti, professionisti della digitalizzazione, manager dell'innovazione digitale e così via).**

Qui di seguito **provo allora a riportare le prime domande sul documento nativo digitale a cui è importante rispondere**. Infatti, quale può considerarsi oggi il "vero documento nativo digitale"? E per il documento nativo digitale quale percorso va sviluppato tale da disegnarvi i nostri processi rilevanti?

- ✓ È realmente **documento nativo digitale** il documento redatto in un formato "testo" in modo da poter essere utilizzato in modo simile al documento cartaceo, o il formato strutturato registrato in modo affidabile che preservi le correlazioni del testo che contiene?
- ✓ Il **futuro della conservazione della memoria digitale** sarà affidato a precisi formati documentali custoditi in modo (più o meno) tradizionale o sempre di più a metadati dinamici contenenti i campi essenziali (es. stringhe di caratteri, sia per i valori dei campi sia per i loro descrittori che sarebbero in grado di ricostruire dinamicamente il layout del documento in ogni momento) da registrare in modo affidabile nel tempo attraverso custodie ininterrotte a livello informatico?
- ✓ E l'**autenticità**, quindi, nei contesti digitali si può perseguire ancora con un'attenzione alla forma documentale o invece dobbiamo necessariamente concentrare le nostre riflessioni sulle registrazioni attendibili di contenuti rilevanti sviluppate e garantite sin dalla loro origine da soggetti affidabili?

Non sono domande ovvie, ma vanno affrontate con coraggio e determinazione perché la tecnologia non aspetta e procede comunque, e non sempre occupandosi e preoccupandosi di preservare la memoria digitale autentica e il relativo contesto archivistico.

Note

1 *Dal segnare al consegnare: la formazione progressiva del documento all'interno del contesto (archivistico) digitale*, pubblicato sul n.1/16 della Rivista KnowIT e su Pubblica Amministrazione 24 del Sole 24 Ore.

2 Come recentemente dichiarato dal Prof. Donato Limone di Unitelma Sapienza durante una riunione del GdL Anorc Professioni dedicato alla governance digitale nelle PA centrali.

3 Emblematico in tal senso è il nuovo comma 2-septies inserito recentemente nell'art. 64. D. Lgs. 82/2005 (come modificato, appunto, dal D. Lgs. 179/2016) nel quale si prevede che "un atto giuridico può essere posto in essere da un soggetto identificato mediante SPID, nell'ambito di un sistema informatico avente i requisiti fissati nelle regole tecniche adottate ai sensi dell'articolo 71, attraverso processi idonei a garantire, in maniera manifesta e inequivoca, l'acquisizione della sua volontà".

4 Così Paul Gabriele Weston, Emmanuela Carbè, Primo Baldini in *Se i bit non bastano: pratiche di conservazione del contesto di origine per gli archivi letterari nativi digitali*. Il pdf è scaricabile direttamente dal sito della rivista open access: https://bibliothecae.unibo.it/index.

5 Termine coniato da Gianni Penzo Doria in "Conservazione digitale, la nuova sfida è il documento senza formati" pubblicato su Forum PA il 07/12/2016 e acquisibile alla pagina http://www.forumpa.it/pa-digitale/conservazione-digitale-la-nuova-sfida-e-il-documento-senza-formati

6 "Documento elettronico: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva" (Regolamento eIDAS - REGOLAMENTO UE N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE).

7 "Documento informatico: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (C.A.D., art. 1, comma 1°, lett. p).

8 Si può licenziare un dipendente con un sms o un messaggio WhatsApp? Info su https://www.laleggepertutti.it/166551_si-puo-licenziare-un-dipendente-con-un-sms-o-whatsapp.

9 Ovvio che a tal proposito oggi qualsiasi impresa o studio professionale (ma anche PA) non può NON interessarsi di proteggere i propri dati giuridicamente rilevanti in un'organizzazione complessa e coerente con quanto la normativa prevede in materia di digitalizzazione e privacy.

10 Forse non ha proprio più senso utilizzare ancora il termine "forma scritta" per il contesto digitale sostituendola, ad esempio, con forma digitale affidabile.

Documenti di identità o di viaggio elettronici: come si utilizzano e quali sono i vantaggi

Alessandro Alessandroni - *Esperto di biometria e documenti elettronici, coordinatore dal 2003 al 2013 del Centro di Competenza sulle tecnologie biometriche di AGID*

La necessità dell'identificazione certa (certezza di identità) delle persone è stata accentuata dai recenti cambiamenti geopolitici, soprattutto in rapporto agli aspetti di sicurezza nazionale.

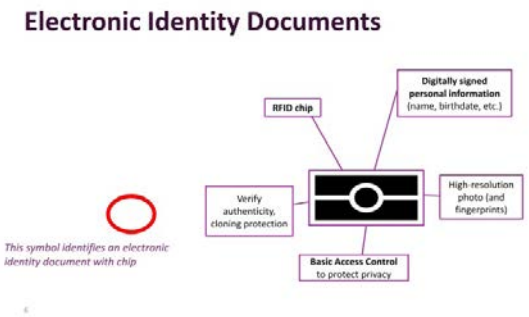
Ma l'esigenza della gestione sicura dell'identità è presente in tutte le altre situazioni nelle quali si deve validare l'identità anagrafica di un cittadino/cliente, indipendentemente dal suo Paese di origine.

Basti pensare a tutte quelle procedure riguardanti i servizi ai quali un cittadino vuole accedere e che prevedono una necessaria fase di verifica dell'identità: l'apertura di un conto corrente bancario, la concessione di un fido finanziario, l'attivazione di una polizza assicurativa, l'acquisizione contrattuale del servizio di una utility e così via.

Partendo dalle specifiche tecniche definite dall'ICAO (*International Civil Aviation Organization*) nel DOC 9303 (https://www.icao.int/publications/pages/publication.aspx?docnum=9303) per i documenti di identità e di viaggio elettronici e dalle prescrizioni di alcune istituzioni sovranazionali quali l'Unione Europea, gli Stati nazionali hanno iniziato a emettere documenti di identità e di viaggio elettronici nell'ottica di poterne poi **effettuare automaticamente, con apposite piattaforme tecnologiche, la lettura** (ovvero l'acquisizione dei dati anagrafici, che ancora si fa con la semplice lettura di un documento tradizionale) **e la relativa validazione di autenticità, insieme alla verifica del titolare**, cosa impossibile da farsi con i documenti di identità tradizionali.

Fatta questa premessa, cerchiamo di capire cos'è un documento di identità o di viaggio elettronico, com'è strutturato e i vantaggi che offre rispetto ai documenti tradizionali.

Come già detto i nuovi documenti elettronici fanno riferimento al DOC 9303 dell'ICAO, si contraddistinguono per il logo rettangolare presente sul fronte del documento (vedi immagine seguente) e comprendono le seguenti tipologie:



- **passaporti elettronici**, emessi da oltre 125 Stati nel mondo per un totale di oltre un miliardo di documenti in circolazione;
- **permessi di soggiorno elettronici**, emessi da tutti gli Stati membri dell'Unione Europea;
- **carte di identità elettroniche** emesse da alcuni Stati, inclusa l'Italia (nuova CIE 3.0 emessa dal 2016).

Attualmente lo Stato italiano ha emesso circa 500.000 carte di identità elettroniche (CIE) e sarebbe certamente utile incoraggiare - se non obbligare - i cittadini italiani a sostituire i loro documenti di identità cartacei con questo nuovo documento.

Il DOC 903 ICAO prevede alcune caratteristiche obbligatorie e alcune caratteristiche opzionali. Tutti i documenti elettronici conformi al DOC 9303 ICAO sono dotati di **due elementi essenziali, una zona denominata MRZ** (*Machine Readable Zone*) costituita da righe orizzontali (due sui documenti di formato maggiore, quali i passaporti, e tre sui documenti in formato smart card) di caratteri di tipo OCR-B per la lettura ottica dei dati, **e un chip RFID** conforme allo standard ISO/IEC 14443.

In entrambi questi elementi (MRZ e chip RFID) sono contenuti sia i dati anagrafici del cittadino che i dati relativi al documento.

Nel chip RFID sono presenti anche gli elementi biometrici: obbligatoria è l'immagine del volto, opzionali le impronte digitali o le immagini dell'iride.

Tutti i dati presenti nel chip devono essere firmati digitalmente dal DS (*Digital Signer*) dell'Autorità di emissione (Ministero dell'Interno nel caso dell'Italia) per garantire integrità e autenticità dei dati; il certificato del DS, presente nel chip, è a sua volta firmato digitalmente dalla **CSCA (*Country Signing Certification Authority*)** dell'Autorità di emissione; la verifica congiunta della firma digitale dei dati e del certificato del DS è denominata ***Passive Authentication (PA)*** e consente di verificare in modo certo l'autenticità e integrità dei dati presenti nel chip.

Nel caso dei passaporti e dei permessi di soggiorno emessi dagli Stati membri dell'UE, è obbligatoria la presenza, oltre all'immagine del volto, anche delle immagini di due impronte digitali. Stessa scelta è stata effettuata dal Ministero dell'Interno per la nuova CIE 3.0. Sono anche presenti meccanismi di sicurezza per:

- verificare che il chip non sia clonato, ***Chip Authentication (CA)*;**
- consentire la lettura delle impronte digitali solo ai soggetti autorizzati dalle Autorità di emissione, ***Terminal Authentication (TA)*;**
- evitare la lettura non autorizzata del chip contactless, consentendone la lettura solo previa acquisizione da parte del dispositivo di controllo delle informazioni presenti nella MRZ e cifrando le comunicazioni tra chip e dispositivo, ***Basic Access Control (BAC)*** o ***Supplemental Access Control (SAC)*** nella forma più evoluta.

I certificati necessari per la verifica dell'autenticità e integrità dei dati presenti nei documenti elettronici emessi dall'Italia (CIE 3.0, passaporto e permesso di soggiorno) sono pubblicati sul portale Internet del Ministero dell'Interno (http://csca-ita.interno.gov.it/index_ITA.htm)[1].

I certificati necessari per la verifica dei passaporti degli altri Paesi sono disponibili attraverso il servizio PKD dell'ICAO (https://www.icao.int/Security/FAL/PKD/Pages/default.aspx) o tramite scambi bilaterali tra Paesi.

Per maggiori dettagli sulle caratteristiche della CIE e del processo di emissione si rimanda alle regole tecniche CIE 3.0 – Specifiche Chip, v.1.0, 25/11/2015 e al Decreto 23 dicembre 2015 "Modalità tecniche di emissione della Carta d'identità elettronica" (GU Serie Generale n. 302 del 30/12/2015).

Conclusioni

I **vantaggi** dei documenti di identità e di viaggio elettronici rispetto ai documenti senza chip consistono nell'**incremento dei livelli di sicurezza**, per la presenza sia di elementi di sicurezza tradizionali che di elementi di sicurezza di tipo crittografico, e nella **possibilità di automatizzare i processi di verifica del documento**. La presenza degli elementi biometrici rende inoltre possibile la verifica automatica anche della identità del titolare. L'aderenza di un documento agli standard ICAO ne consente la verifica con gli stessi sistemi di controllo, indipendentemente dal tipo di documento (passaporti, carte di identità, permessi di soggiorno etc.) e dal Paese di emissione.

Le modalità di verifica comprendono **varchi automatici e postazioni fisse alle frontiere, postazioni mobili utilizzate dalle forze di polizia** sul territorio ma anche **dispositivi utilizzati per le verifiche di identità da soggetti che hanno l'esigenza di verificare l'identità del cliente** per l'erogazione di un servizio.

Usando lettori fissi o mobili con l'opportuno software, in pochi secondi anche soggetti non esperti possono verificare l'autenticità e l'integrità del documento e quindi l'identità del titolare tramite riconoscimento biometrico della foto (le impronte sono verificate solo da soggetti autorizzati dall'Autorità di emissione).

Si stanno affermando **soluzioni software che possono essere installate su qualsiasi apparato Android dotato di funzionalità NFC**, consentendo l'automazione della lettura dei dati riportati sui singoli documenti congiuntamente alla verifica di autenticità.

La possibilità offerta da queste soluzioni di completa automazione della lettura del documento, unita alla conferma di autenticità del documento stesso, ne fanno un indispensabile strumento per la gestione di molte procedure in ambito pubblico e privato, per semplici finalità commerciali o per aumentare le procedure di sicurezza in molteplici contesti. Basti pensare a tutte quelle procedure nelle quali ancora oggi i dati anagrafici vengono acquisiti in modalità manuale, con dispendio di tempo, possibilità di errori di data-entry e difficoltà per un soggetto non esperto di verificare a vista l'autenticità di un documento.

Alcune app, dopo la verifica dell'autenticità del documento, consentono anche la verifica biometrica (volto) del titolare, comparando la foto digitale presente nel chip dei documenti elettronici con una foto o con un selfie acquisito al momento.

La verifica può essere effettuata da operatori in modalità *face2face* per verificare l'autenticità dei documenti presentati o dagli stessi utenti di servizi on line per dimostrare l'autenticità dei propri documenti.

Note

1 La chiave pubblica della CSCA Italiana viene utilizzata per verificare l'autenticità del certificato del DS dopo aver verificato che i dati nel chip siano stati firmati dal DS. La CSCA è unica per tutti i documenti, mentre i DS sono diversi per i tre tipi di documento.

Controlli a distanza e web-sorveglianza dei lavoratori: tra novità normative e variazioni ermeneutiche (Prima parte)[1]

Angela Busacca - *Ricercatore Universitario - Docente di Diritto dell'Informatica, Università "Mediterranea" di Reggio Calabria*

Tra i temi più dibattuti e più sensibili all'evoluzione tecnologica in relazione alle dinamiche dei rapporti di lavoro, la questione dei limiti di liceità dei cd. controlli a distanza da parte del datore di lavoro rappresenta indubbiamente uno degli argomenti più "scottanti", come testimoniano i fermenti normativi degli ultimi anni (in particolare le modifiche apportate all'art. 4 dello Statuto dei lavoratori con i decreti attuativi del Jobs Act) e gli interventi della giurisprudenza di merito e di legittimità che si è trovata a pronunciarsi sulla individuazione del discrimine tra esercizio (legittimo) del controllo e tutela della sfera di riservatezza dei lavoratori. **La stessa espressione "controlli a distanza" compendia una pluralità di situazioni che**, come emerge dalla nuova formulazione**, si riferiscono sia alle attività di controllo sui dispositivi** che possono essere utilizzati nello svolgimento dell'attività lavorativa (*pc, gps, smartphone* e altre tipologie di *device*) **sia alla installazione e all'utilizzo di strumenti di videoripresa** che permettono il monitoraggio delle attività e la registrazione e archiviazione dei filmati: appare dunque manifesto come l'evoluzione tecnologica determini uno sviluppo in senso sia qualitativo che quantitativo delle possibilità di controllo e al contempo possa implicare una maggiore ingerenza nella sfera privata dei lavoratori. In particolare, proprio in relazione a questo ultimo profilo **si segnala la sentenza della Corte di Cassazione, sez. III penale, 8 maggio 2017 n. 22148, che ha determinato una inversione di tendenza** rispetto alla impostazione maggioritaria (quella indicata dalla cd. sentenza "Banti" del 2012) in tema di controllo a distanza attraverso strumenti di videoripresa ed efficacia scriminante del consenso individuale prestato dai lavoratori, in assenza di previo accordo con le rappresentanze sindacali o di preventiva autorizzazione da parte della DTL.

L'art. 4 dello Statuto dei lavoratori prevedeva, nella sua formulazione pre-novella, il divieto di "uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", temperando poi la rigidità della previsione con la possibilità di installazione di "impianti e apparecchiature di controllo" previo accordo con le rappresentanze sindacali aziendali (o, in mancanza di esse, con la commissione interna), quando tali impianti risultassero finalizzati a "esigenze organizzative e produttive" ovvero motivati da ragioni di sicurezza del lavoro: già a una prima lettura "con gli occhiali del nuovo millennio" e della evoluzione tecnologica, la norma denuncia tutta la propria insufficienza a regolare i diversi aspetti della comunicazione *on line* e della gestione e trattamento della mole di dati personali raccolti tramite i controlli a distanza. **Le modifiche apportate dall'art.23 del d.lgs. 151/2015 hanno ridisegnato la geografia interna dell'art.4 dello Statuto dei lavoratori** (oggi rubricato semplicemente "Impianti audiovisivi"), individuando due distinti "nuclei normativi" relativi ai controlli a distanza (comma I e II) e all'utilizzo dei dati raccolti lecitamente per tutte le finalità connesse al rapporto di lavoro (comma III). Tra le innovazioni più significative, deve segnalarsi in primo luogo il diverso approccio scelto dal legislatore: **non più un generale divieto poi temperato dalle ipotesi "eccezionali", bensì la previsione espressa dell'impiego per finalità determinate e in presenza di preventivo accordo**. Nell'ambito delle novità, ancora, deve evidenziarsi come, tra le finalità, viene indicata anche la tutela del "patrimonio aziendale" (recependo così gli esiti di quella giurisprudenza che aveva ammesso la legittimità dei cd. controlli difensivi), e come, in relazione agli strumenti di controllo, **vengono individuati i due distinti momenti della installazione e dell'utilizzo degli stessi**: per l'installazione viene posto come prerequisito essenziale l'accordo collettivo stipulato dalla RSU o dalle RSA (oppure, in ipotesi di imprese con unità produttive ubicate in più provincie della stessa regione o in più regioni, con accordo stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale) o, in assenza di esso, con autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro (o della sede centrale in ipotesi di impresa con diverse sedi produttive).

L'installazione e l'impiego degli strumenti per il controllo a distanza determinano, seppur effettuati nell'ambito delle finalità indicate dalla norma, una ingerenza nella sfera privata del lavoratore e determinano **l'acquisizione, da parte del datore, di una serie di dati per il trattamento dei quali devono essere rispettate le previsioni** e i principi **del d.lgs.196/2003** (cd. codice privacy): in particolare, in ipotesi di utilizzo illecito degli strumenti e di attività di trattamento svolte in violazione delle norme del codice della privacy, vengono in considerazione le ipotesi di illecito previste dagli artt.114 e 171 del d.lgs. 196/2003, che per certi versi si pongono in una linea di continuità con quanto previsto dallo Statuto dei lavoratori. In particolare, l'ipotesi di illiceità che viene in considerazione con riferimento all'installazione degli apparecchi, riguarda la mancanza di preventivo accordo o di autorizzazione: sul punto, tuttavia, si è posto il dubbio se l'eventuale consenso scritto, prestato da tutti i lavoratori interessati dalla videoripresa, potesse avere valore sostitutivo e rendere così legittimo il posizionamento e l'utilizzo dell'impianto. Nel silenzio del legislatore sul punto, posta l'assenza anche di un semplice richiamo al valore del consenso del lavoratore, prestato ai sensi e con le modalità previste dal d.lgs. 196/2003, la Corte di Cassazione aveva proposto, con la cd. "sentenza Banti" del 2012, una ricostruzione tesa a valorizzare l'autonoma determinazione dei singoli, riconoscendo valore scriminante al consenso prestato dai lavoratori; tuttavia tale orientamento è stato capovolto, come anticipato, con **la recentissima sentenza della Corte di Cassazione 8 maggio 2017, n. 22148** che **ha riaffermato il valore dell'accordo come forma di codeterminazione** che supera le volontà individuali e si pone come maggiormente rappresentativa di un interesse superindividuale dei lavoratori.

Con la sentenza 17 aprile 2012, n, 22611 (cd. sentenza Banti), la Corte di Cassazione aveva proposto una lettura tesa alla valorizzazione della dimensione individuale del consenso, affermando la natura scriminate del consenso prestato dai lavoratori; in sostanza, pur in assenza di accordi o autorizzazioni preventive, come richiesto dall'art.4 dello Statuto dei lavoratori, il datore non poteva ritenersi penalmente responsabile per l'installazione di strumenti di controllo a distanza, posto il valore del consenso dato dai lavoratori interessati, i quali non solo dimostravano di essere a conoscenza delle attività di videosorveglianza e videoripresa, ma avevano dato il proprio consenso alle (connesse) attività di trattamento dati ex d.lgs. 196/2003. In particolare la Corte aveva accordato valore prevalente alla dimensione individuale, ponendo in primo piano il principio di autodeterminazione della persona in ordine al consenso sulle attività di trattamento dei dati e ritenendo prevalente il consenso prestato dai diretti interessati rispetto a quello di una rappresentanza ("tale consenso deve essere considerato validamente prestato quando promani proprio da tutti i dipendenti, posto che l'esistenza di un consenso validamente prestato da parte di chi sia titolare del bene protetto, esclude la integrazione dell'illecito"). Sul portato di questa interpretazione, tuttavia, appare chiaro come potrebbe realizzarsi, di fatto, un superamento della procedura (e delle garanzie offerte) ex art.4 dello Statuto dei lavoratori, posto che il lavoratore potrebbe prestare il proprio consenso non tanto e non solo in forza di una autodeterminazione consapevole, ma (altresì) in conseguenza di una posizione di debolezza contrattuale che lo espone alle determinazioni del datore. Proprio su questa linea interpretativa e, valorizzando il ruolo della (preventiva) codeterminazione tramite accordo o della autorizzazione DTL, la Corte di Cassazione ribalta, a cinque anni di distanza, la propria linea interpretativa, affermando la rilevanza penale della condotta illecita del datore.

La vicenda in questione prende avvio dalla installazione di uno strumento di controllo (impianto di videoripresa con due telecamere – una su un'area adibita a magazzino, l'altra sull'area della cassa - collegate a dispositivo wi-fi e monitor in grado di trasmettere le immagini riprese), fatta dal titolare di un esercizio commerciale in assenza di accordo (preventivo) o autorizzazione DTL, ma in presenza di consenso, manifestato oralmente, da parte di tutti i lavoratori (che, peraltro, nel corso del giudizio di merito avevano testimoniato in tal senso, affermando non solo di essere a conoscenza dell'installazione dell'impianto, ma altresì di aver dato il proprio consenso in forma orale). Tale consenso, tuttavia, non veniva considerato validamente scriminante dal Tribunale di Terni che condannava il datore al pagamento di un'ammenda di euro 600; avverso tale sentenza ricorreva il datore, asserendo l'insussistenza del reato, sul portato della presenza di un consenso (scriminante) prestato dai lavoratori.

La Corte di Cassazione, come già anticipato, con la sentenza 8 maggio 2017, n. 22148, non accoglie la doglianza e anzi **evidenzia come non possa riconoscersi alcun valore scriminante al consenso prestato dai lavoratori, riconducendo a diversi piani di interesse e di relativa tutela il ruolo del consenso individuale e del consenso espresso (dalle rappresentanze sindacali) in sede di accordo**. In particolare, la Corte di Cassazione afferma come "non abbia alcuna rilevanza il consenso scritto o orale concesso dai singoli lavoratori, in quanto la tutela penale è apprestata per la salvaguardia di interessi collettivi di cui, nel caso di specie, le rappresentanze sindacali, per espressa disposizione di legge, sono portatrici, **in luogo dei lavoratori che, a causa della posizione di svantaggio nella quale versano rispetto al datore di lavoro, potrebbero rendere un consenso viziato"**; difatti, posto che "la norma penale in discorso tutela interessi di carattere collettivo e superindividuale", appare manifesto come "la condotta datoriale, che pretermette l'interlocuzione con le rappresentanze sindacali unitarie o aziendali procedendo all'installazione degli impianti dai quali possa derivare un controllo a distanza dei lavoratori, produce l'oggettiva lesione degli interessi collettivi di cui le rappresentanze sindacali sono portatrici, in quanto deputate a riscontrare, essendo titolari ex lege del relativo diritto, se gli impianti audiovisivi, dei quali il datore di lavoro intende avvalersi, abbiano o meno, da un lato, l'idoneità a ledere la dignità dei lavoratori per la loro potenzialità di controllo a distanza, e di verificare, dall'altro, l'effettiva rispondenza di detti impianti alle esigenze tecnico-produttive o di sicurezza in modo da disciplinarne, attraverso l'accordo collettivo, le modalità e le condizioni d'uso e così liberare l'imprenditore dall'impedimento alla loro installazione". Su questa linea interpretativa, peraltro, l'illecito datoriale viene ricondotto altresì all'alveo delle condotte antisindacali, richiamando anche la specifica tutela ex art.28 dello Statuto dei lavoratori.

Del resto il mutato orientamento interpretativo, maturato anche a seguito della novella apportata con il *Jobs Act*, può leggersi anche nell'affermazione del Tribunale di Milano, che nella recentissima sentenza del 10 febbraio 2017, ha riconosciuto la violazione dell'art.4 dello Statuto dei lavoratori anche in caso in installazione di impianto, in assenza della procedura richiesta, pur in presenza della circostanza fattuale della inattività dell'impianto stesso, ma in forza della "idoneità potenziale" a essere utilizzato per finalità di controllo[2].

Note

[1] La seconda parte del contributo verrà pubblicata nel prossimo numero della rivista e tratterà delle diverse questioni inerenti all'utilizzo dei *pc* e dei *device* e della possibilità di controllo dei contenuti da parte del datore di lavoro.

[2] Trib. Milano 10.02.2017 (banca dati e.pluris on line): "ai fini della violazione del disposto di cui all'art. 4 della legge n. 300 del 1970 (Statuto dei Lavoratori), è sufficiente la potenziale idoneità dei dispositivi al controllo a distanza dei lavoratori, senza la preventiva attivazione della procedura prevista dalla medesima norma. Di talché non assume alcun rilievo, in senso contrario, la circostanza che al momento del controllo i dispositivi in parola risultino inattivi".

Direttiva eIDAS (EU 910/2014) e direttive italiane in materia di digitalizzazione

Fabrizio Cirilli - *Lead auditor eIDAS e amministratore unico PDCA Srl*
Riccardo Bianconi - *Business & Team Coach, Management systems auditor and designer, auditor IT e Ispettore di ACCREDIA*

Di cosa si tratta

Per una efficace sintesi degli obiettivi, del significato e degli impatti del Regolamento (UE) 910/2014 - eIDAS nel nostro Paese ci rifacciamo a quanto descritto nel sito AgID:
"Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri […]. Il regolamento, "allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari:

- fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche […];
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web […].

In quest'ottica, particolare rilevanza assume anche la piena interoperabilità a livello comunitario di particolari tipologie di firme elettroniche e dei sistemi di validazione temporale note in Italia rispettivamente come firma digitale e marca temporale […].
In conclusione, con l'attuazione a livello comunitario del regolamento eIDAS in tutti i settori, si tenderà alla creazione di un mercato unico digitale che:

- semplifichi l'accesso alle pubbliche amministrazioni;
- favorisca la trasformazione digitale delle organizzazioni ed imprese;
- stimoli lo sviluppo di servizi innovativi e sicuri;
- contribuisca a snellire e semplificare gli adempimenti amministrativi e burocratici;
- migliori l'esperienza digitale degli utilizzatori e stimola la fornitura di nuovi e innovativi servizi.

Il regolamento eIDAS è stato emanato il 23 luglio 2014 e ha piena efficacia dall'1 luglio del 2016."

Introduzione

A giugno dello scorso anno, con uno sforzo significativo, **l'Italia ha avviato il processo di attuazione previsto nel Regolamento (UE) 910/2014 - eIDAS per quanto concerne la marcatura temporale**. Poi, nei mesi successivi**, è stata attivata anche la parte inerente alla firma digitale, seguita dalle direttive italiane sulla conservazione e il sistema di identificazione nazionale SPID**.
Si tratta di processi complessi che hanno coinvolto diverse "parti interessate" e che hanno condotto l'Italia a essere uno dei primi paesi europei (se non il primo) a dotarsi del sistema di certificazione accreditata dei prestatori di servizi fiduciari (o più brevemente TSP) e dei servizi eIDAS previsti dalla direttiva.
I principali attori del processo sono stati:

- ETSI (per quanto riguarda gli standard per la definizione tecnico organizzativa dei TSP e dei servizi);
- AgID (per quanto riguarda l'attuazione e la concertazione nazionale);
- ACCREDIA (per quanto concerne i processi di accreditamento nazionale degli organismi di certificazione e della qualifica degli *auditor*);
- gli Organismi di Certificazione, accreditati da ACCREDIA nell'ambito della sicurezza delle informazioni secondo la ISO/IEC 27001:2013 (per quanto riguarda le attività di verifica sul campo);
- UNINFO (per quanto riguarda il supporto alla normazione tecnica).

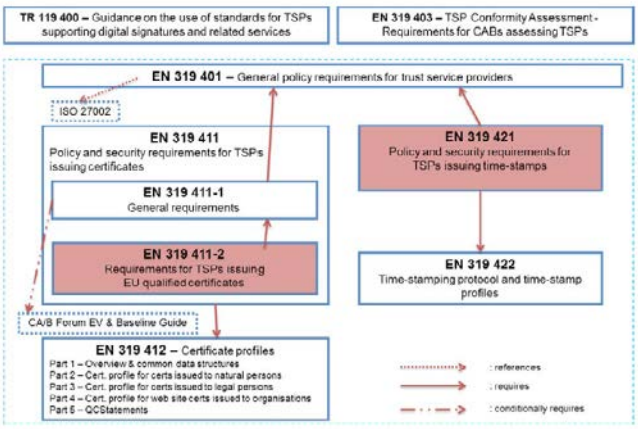
Ovviamente il "progetto" era già in corso da tempo e solo nella fase finale ha riunito tutti i soggetti per il primo corso di qualifica di un gruppo iniziale di *auditor*, individuati secondo competenze specifiche nel settore della sicurezza delle informazioni e nell'ICT.
Abbiamo avuto il privilegio di essere in questo gruppo e di far parte dei primi gruppi di *audit* sul territorio nazionale, da questa esperienza scaturiscono le considerazioni che seguono in questo articolo in cui intendiamo condividere un'esperienza pratica (ancora in corso) vista dalla prospettiva di chi lavora sul campo e cerca di far "quadrare" gli standard, le leggi e le direttive con la vita delle aziende che vengono sottoposte ad *audit*.
I riferimenti tecnici e normativi: una nuova situazione
Primo e forse più ostico argomento sono gli standard tecnici ETSI e gli articoli del Regolamento (UE) 910/2014 - eIDAS, resi attuabili grazie al lavoro svolto da AgID e ACCREDIA. Ostici perché si tratta di argomenti nati in momenti diversi, quindi non "progettati" per essere verificati e sottoposti ad *audit*, almeno per come siamo abituati dal mondo delle certificazioni ISO.
Ad esempio, l'*audit* di certificazione di un TSP prevede sia una componente di sistema (basata sulla ISO/IEC 17021, come la certificazione di un sistema di gestione ISO/IEC 27001, per intenderci), sia una componente di prodotto (basata sulla ISO/ICE 17065, normalmente riservata a prodotti e apparati).
Questo è il primo fattore di complessità che tutte le parti interessate (TSP in testa) si sono trovati ad affrontare. **Per la prima volta una direttiva europea si trasforma in un *audit* "combinato" a due dimensioni e velocità: sistema e prodotto anziché l'uno o l'altro**.
Le aziende sono abituate ad *audit* del genere, visto che il mercato ICT è pieno di casi simili, ma **mai un numero così rilevante di aziende italiane si sono trovate a dover conseguire una certificazione di questo tipo, e per giunta obbligatoria, pena l'esclusione dai servizi e dalle relative liste autorizzative di AgID**.
Anche il meccanismo di certificazione è stato modificato: l'ultima parola spetta ad AgID e non all'organismo di certificazio-

ne, che in questo caso diventa un mezzo (sebbene fondamentale) per il processo di accreditamento verso AgID. ACCREDIA ha seguito da vicino tutti gli Organismi di Certificazione, secondo le regole vigenti di accreditamento, con un particolare focus su ogni servizio oggetto di certificazione.
Quindi lo scenario è: aziende già inserite nelle liste autorizzative AgID che si devono sottoporre a un nuovo *audit* secondo standard internazionali di sistema e prodotto, entro date strettissime prestabilite, ***audit* fattibile solo dai pochi Organismi** che hanno partecipato alle sessioni formative indette da ACCREDIA, con la collaborazione di AgID e a cura di rappresentanti di ENISA e ETSI. Pena l'esclusione dalle liste AgID e/o la perdita della validità del servizio di marcatura temporale.
È facilmente immaginabile quale sia stata la corsa alla preparazione, organizzazione e conduzione dei primi *audit* di certificazione, in prima istanza condotti da due organismi di certificazione, poi diventati cinque nei mesi successivi. Ad oggi altri Organismi di Certificazione sono in fase di accreditamento in modo da ampliare l'offerta e le potenzialità di questo mercato.

Dal lato delle aziende

Da parte delle aziende (TSP) c'è stato un momento di smarrimento dovuto al fatto che **l'Organismo di Certificazione che aveva rilasciato il certificato obbligatorio ISO/IEC 27001 potesse non essere nella lista degli Organismi qualificati da ACCREDIA per il rilascio delle certificazioni eID**AS. Il che ha portato inevitabilmente a situazioni in cui il TSP, avendo un certificato ISO/IEC 27001 rilasciato da un Organismo A, si è dovuto rivolgere a un Organismo B per la parte eIDAS, con l'esigenza di ripercorrere almeno in parte il processo di valutazione, specialmente sugli aspetti sistemici previsti dalla Norma ESTI EN 319 401, che è una Norma sistemica, al pari della ISO/IEC 27001.
Audit diverso dunque sotto molti punti di vista. I primi TSP non erano consapevoli del cambio di marcia imposto dalla componente di certificazione di prodotto dovuta alla ISO/IEC 17065, quindi in un primo momento vi sono state situazioni di incomprensione, del tutto legittime, risolte grazie al buon senso di tutti e alla professionalità dei soggetti coinvolti.
Significativo il numero di giornate di *audit* svolto sul campo, dovuto proprio alla componente di certificazione di prodotto. Le implicazioni tecniche e tecnologiche sono numerose e la necessità di visitare tutti gli HSM del TSP ha aumentato notevolmente l'*effort* per Organismi di Certificazione e TSP.
ACCREDIA dal canto suo ha cercato di mantenere il passo rispetto alle richieste provenienti da AgID e dai TSP, emettendo una serie di circolari per il progressivo affinamento dei conteggi per il calcolo dei giorni/persona necessari alla certificazione. Ad oggi la situazione appare stabilizzata ma l'estensione ormai attiva della certificazione dei servizi di sigillo, dei siti web, nonché della conservazione di firme e sigilli (altro servizio tipicamente eIDAS) lascia già presupporre la necessità di ulteriori revisioni, soprattutto per la definizione di scenari e combinazioni capaci di soddisfare tutte le possibili richieste tenendo conto delle parti comuni e delle singole specificità e l'esigenza di uno specifico schema per il servizio di conservazione, che si è già deciso di erogare a fronte delle esigenze del mercato.
Il ruolo delle checklist ETSI
AgID, nei mesi precedenti all'avvio delle attività, aveva distribuito ai TSP alcune ***checklist* prodotte dalla ETSI utili all'auto verifica dei requisiti per la certificazione eIDAS**.
Queste *checklist* sono ad oggi (almeno a nostro parere) la chiave di volta dell'intero processo di certificazione.
Le *checklist* **delineano circa un migliaio di requisiti** (spesso fortunatamente ridondati) che costituiscono la struttura portante dell'*audit* di certificazione sia del TSP (lato sistemico) sia dei servizi (lato prodotto).
L'autovalutazione e la compilazione di queste *checklist*, prima dell'avvio del processo di certificazione, si sono rivelati fattori determinanti per il successo dell'intero progetto.
Le *checklist*, evidentemente non progettate per essere utilizzate in questo senso, hanno mostrato da subito alcune lacune (la più evidente è l'**alto numero di ridondanze**) ma si sono comunque subito rivelate come un criterio valido di razionalizzazione e raccolta degli elementi necessari a dimostrare lo stato di "maturità" rispetto alla certificazione dei servizi eIDAS.
Grazie al costante lavoro di ACCREDIA, di AgiD e degli Organismi di Certificazione, ad oggi l'uso delle *checklist* è stato chiarito e tutti gli *auditor* impegnati in campo ne possono apprezzare l'utilità (sebbene le ridondanze rimangano un problema da risolvere a livello ETSI).
Per lo specifico schema Conservatori a Norma, che è uno schema del tutto nazionale da non confondere con la conservazione di firme e sigilli prima richiamata, l'uso della *checklist* di AgID è ancora il cardine del processo di certificazione. Tale strumento è destinato a una revisione che le parti interessate hanno deciso di avviare a fine estate, sulla base delle esperienze maturate. Decisione presa in occasione dell'ultimo Forum Conservatori, organizzato da AgID.
Vista la complessità degli strumenti di valutazione, il suggerimento per i TSP dettato dall'esperienza è: sottoponetevi a un'autovalutazione preliminare utilizzando e completando le *checklist* con tutti i riferimenti (documentali e tecnici), in modo da poter valutare in assoluta autonomia e tranquillità il vostro stato di adeguatezza prima di attivare il contratto di certificazione. In alcuni casi la distanza dal profilo minimo o l'errore interpretativo hanno condotto a un allungamento significativo dei tempi di certificazione o a situazioni spiacevoli nel corso dell'*audit*.
Di fatto gli *audit* eIDAS non sono come gli *audit* di certificazione per la ISO/IEC 27001 e talvolta non hanno neanche lo stesso "campo di applicazione", per questo ci sentiamo di raccomandare a tutti i TSP interessati un'attenta lettura della direttiva e dei documenti reperibili sia sul sito AgID sia sul sito ACCREDIA.

Facciamo un esempio per chiarire il punto: spesso la valutazione dei rischi utilizzata per la certificazione ISO/IEC 27001 raggruppa i servizi del TSP, mentre è assolutamente evidente che la valutazione dei rischi deve riferirsi (o almeno permettere di isolare) i servizi eIDAS oggetto di certificazione. In almeno un caso (tra quelli noti ad oggi) ciò ha comportato la ridefinizione del processo di valutazione del rischio e quindi la sua ripetizione, con evidenti differenze rispetto alla precedente versione con i servizi aggregati.
È chiaro, **quindi, che anche la consapevolezza del TSP viene modificata applicando le *checklist* e le direttive, con un effetto sicuramente positivo ai fini della sicurezza**.
Un ulteriore esempio della crescita della consapevolezza degli operatori TSP si riscontra circa il servizio nazionale di conservazione a norma, ove la logica di analisi dei processi dati in *outsourcing* viene totalmente rivisitata e l'approccio di servizio deve fare i conti con un livello di responsabilità e con un rigore dell'*audit* ben diverso da quello incontrato in ambito volontario. Non si tratta di diversi livelli di serietà professionale, ma di diversi livelli di garanzia, che prevedono campionamenti sicuramente più significativi.
Di contro, alcuni casi limite portano a riflettere sulle attuali modalità di svolgimento degli *audit*, ancora un esempio tratto dall'esperienza in campo: quando un HSM di proprietà del cliente e contenuto in un *data center* dello stesso ha a bordo un certificato emesso dal TSP occorre che l'*audit* raggiunga questo apparato per verificarne alcuni requisiti specifici. È immaginabile la complessità burocratica e logistica di recarsi presso siti del cliente finale (del TSP). Anche in questo caso le aziende italiane e i loro clienti si sono rivelate assolutamente disponibili e aperte dimostrando l'alto livello di professionalità e sicurezza delle infrastrutture utilizzate.
A titolo puramente informativo riportiamo **lo schema degli standard ETSI oggetto di *audit*:**



Ne risulta evidente la complessità e l'interdipendenza a livello strutturale: le ripercussioni per *auditor* e TSP sono facilmente immaginabili.

Conservazione e SPID

Subito dopo l'attivazione dei servizi eIDAS le "parti interessate" hanno dato il via alle medesime attività per due dei servizi nazionali di maggior rilievo nell'ambito della digitalizzazione: la conservazione e lo SPID.
Anche in questo caso AgID e ACCREDIA hanno attivato un corso di formazione e qualifica per gli *auditor* degli Organismi di Certificazione, corso propedeutico e vincolante (al pari di quello eIDAS) per poter eseguire *audit* di certificazione di questi due servizi. La differenza principale è che **in questo caso non vi sono standard ETSI a supporto ma documenti prodotti da AgID**.
I tempi erano ovviamente diversi da quelli fissati da eIDAS pertanto questi servizi sono partiti in momenti successivi e hanno in qualche modo beneficiato delle esperienze maturate per eIDAS.
Trattandosi di ambito nazionale e di direttive in larga parte già note e attuate lo sforzo è stato minore ma non meno interessante e pieno di punti di riflessione e discussione, come già sopra evidenziato. Ad esempio è stata rivalutata in corsa la necessità **che un conservatore risponda anche a parte delle direttive ETSI** inizialmente richiamate per similitudine e continuità con i servizi eIDAS. Questo ha significativamente ridotto la complessità, e quindi la durata, degli *audit* in campo ed ha condotto alla stesura (da parte di AgID) di apposite *checklist*, più orientate alla verifica dei servizi specifici secondo le esigenze nazionali.

Situazione attuale

Purtroppo, per vari problemi di natura tecnica e burocratica, **non risulta facile per un utente finale capire chi è certificato e accreditato e per quali dei servizi eIDAS e nazionali**, non essendo ancora disponibile un punto di raccolta unico a livello internazionale e nazionale.
Il sito AgID fornisce l'elenco degli Organismi di Certificazione accreditati per i servizi eIDAS e nazionali:

Organismi di valutazione accreditati (Regolamento CE 765/2008)	Servizi autorizzati			
	Valutazione dei gestori di identità digitale SPID	Valutazione dei prestatori di servizi fiduciari qualificati per l'emissione di certificati qualificati in ambito eIDAS	Valutazione dei prestatori di servizi fiduciari qualificati per l'emissione di marche temporali qualificate in ambito eIDAS	Valutazione dei soggetti accreditati per i sistemi di conservazione documentale
BUREAU Veritas Italia	Si	Si	Si	Si
Certiquality	No	Si	Si	No
CSQA Certificazioni	No	Si	Si	Si
DNV GL Business Assurance Italia	Si	Si	Si	Si
IMQ	No	Si	Si	No
KIWA Cermet Italia	No	Si	Si	No
RINA Services	No	No	No	Si

Data ultimo aggiornamento: 13 luglio 2017

La lista dei TSP che hanno superato l'*audit* di certificazione, invece, non è ancora facilmente raggiungibile, a livello sia nazionale che europeo, ed è in una fase dinamica di raccolta informazioni.

Conclusioni

Nonostante la complessità iniziale il sistema nazionale va via via risolvendo i punti critici e le aziende italiane (TSP e loro clienti) possono finalmente usufruire di servizi digitali in linea con le direttive europee con livelli di sicurezza rispondenti a standard tecnici specifici.
Anche il contributo di ENISA, con alcuni documenti specifici, ha permesso all'Europa di progredire in questo ambito, forse con differenti velocità ma sicuramente in modo efficace.

La Guida del Garante all'applicazione del Regolamento europeo in materia di protezione dei dati personali

Michele Iaselli - *Presidente ANDIP*

La recente Guida del Garante all'applicazione del Regolamento europeo in materia di protezione dei dati personali si rivela sicuramente molto utile, specialmente per tutti coloro che per la prima volta si trovano ad affrontare le prime incertezze e i primi dubbi sorti a seguito dell'avvento del Regolamento.
Indubbiamente, come sostiene la stessa Autorità, **la Guida non può e non vuole essere esaustiva**, **poiché ci saranno molte questioni che potranno essere risolte solo con interventi normativi di carattere nazionale** che, tra l'altro, dovranno essere concordati in ambito comunitario, considerata la natura del Regolamento.
Ci sono, però, alcuni punti fermi che il Garante ha voluto ribadire al fine di chiarire le idee sull'effettiva portata del provvedimento comunitario, che, come è noto, **diventerà obbligatorio per tutti i paesi dell'UE a decorrere dal 25 maggio 2018**.
Innanzitutto viene precisato che i fondamenti di liceità del trattamento indicati all'art. 6 del Regolamento coincidono, in linea di massima, con quelli previsti attualmente dal Codice (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).
Le principali novità in merito al consenso sono che:

- **per i dati "sensibili"** (art. 9 del Regolamento) il consenso **deve essere "esplicito"**; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22);
- **non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta"**, difatti viene precisato dall'art. 7 del Regolamento che il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali. In realtà, però, il Garante continua a ritenere che la forma scritta rimanga la modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili);
- **il consenso dei minori è valido a partire dai 16 anni,** prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Il Garante si esprime anche in merito all'informativa chiarendo che i contenuti sono elencati in modo tassativo negli articoli 13 (paragrafo 1) e 14 (paragrafo 1) del Regolamento e in parte sono più ampi rispetto al Codice.
Il Regolamento, inoltre, specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, **che deve avere forma concisa, trasparente, intelligibile** per l'interessato e **facilmente accessibile**; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee.
L'informativa è data, in linea di principio, **per iscritto e preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online). Il Regolamento ammette, soprattutto, **l'utilizzo di icone** per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'UE e saranno definite prossimamente dalla Commissione europea (formati multistrato).
Sono, inoltre, parzialmente diversi i requisiti che il Regolamento fissa per l'esonero dall'informativa (art. 13, paragrafo 4 e art. 14, paragrafo 5 del Regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (art. 14, paragrafo 5, lettera b)), a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.
Il Garante raccomanda, inoltre, **come sia opportuno che i titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i nuovi criteri** sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.
I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, continuare o iniziare a utilizzare queste modalità per la prestazione dell'informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.), in attesa della definizione di icone standardizzate da parte della Commissione.
Riguardo poi ai diritti degli interessati, il Garante specifica che **il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), un mese, estendibile fino a 3** mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego. Spetta, poi, al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedergli, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive).

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3). La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
Naturalmente il Garante chiarisce che il Regolamento prevede nuovi diritti dell'interessato, come il diritto alla cancellazione e all'oblio (art. 17), il diritto di limitazione del trattamento (art. 18), il diritto alla portabilità dei dati (art. 20).
Riguardo alle figure soggettive, il Garante pone l'accento sul fatto che il Regolamento disciplina la contitolarità del trattamento (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati. Lo stesso Regolamento fissa più dettagliatamente (rispetto all'art. 29 del Codice) **le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: **deve trattarsi**, infatti, **di un contratto** (o altro atto giuridico conforme al diritto nazionale). Inoltre, il Regolamento consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento e prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari.
Viene, inoltre, ribadita dal Garante **l'importanza del principio di *accountability*** accolto dal Regolamento europeo e inteso come l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, nonché **la rilevanza del principio della *privacy by design* e *by default*** inteso come necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del Regolamento (si veda l'art. 39), essendo finalizzata a facilitare l'attuazione del Regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35.
Altro aspetto che il Garante tiene a sottolineare è che, a seguito del Regolamento, l'intervento delle autorità di controllo sarà principalmente *ex post*, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare: ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda l'art. 17 del Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.
Da ultimo la guida dedica particolare attenzione ai trasferimenti di dati verso paesi terzi e organismi internazionali, puntualizzando che in primo luogo **viene meno il requisito dell'autorizzazione nazionale**. Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione (ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento), potrà avere inizio senza attendere l'autorizzazione nazionale del Garante, a differenza di quanto attualmente previsto dall'art. 44 del Codice.
In definitiva, comunque, il Regolamento conferma l'approccio attualmente vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi siano vietati, in linea di principio, a meno che intervengano specifiche garanzie.

Una Polaroid della digitalizzazione nella PA italiana

Chiara Pascali - *Responsabile comunicazione ANORC e ANORC Professioni*

Che la digitalizzazione della PA italiana, seppur avviata da tempo, stenti a decollare è un fatto sotto gli occhi di tutti (quanti di voi riescono già a usufruire dei servizi digitali della PA e quanti ancora no o solo in parte?), ma comprendere bene le dimensioni del problema è di certo un passo importante per avviarsi a trovarne la soluzione. In questa direzione si è mosso il **Gruppo di lavoro sulla Governance** promosso da ANORC e ANORC Professioni, costituito **con l'obiettivo di individuare modelli di governance e competenze utili alla gestione digitale di documenti e informazioni nella PA**.

Con il supporto dei membri del Gruppo di Lavoro, ANORC e ANORC Professioni hanno effettuato una rilevazione[1] per comprendere quale sia il reale stato dell'arte legato agli aspetti dell'innovazione digitale del settore pubblico nel 2016, potendo lavorare su un campione d'indagine di 17 enti pubblici nazionali, rappresentativo di diversi ambiti dell'Amministrazione pubblica (dalla ricerca alla vigilanza del sistema bancario, dall'istruzione allo sviluppo economico, dalla previdenza al conio).

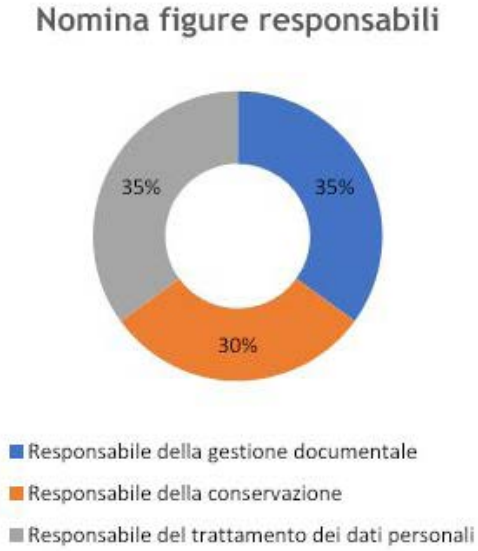
I dati emersi hanno mostrato chiaramente come anche negli enti pubblici centrali (quelli per i quali si potrebbe immaginare che la nuova organizzazione digitale venga applicata per prima e in modo più compiuto) viga ancora un regime di incertezza e alcuni tasselli importanti per completare il meccanismo della digitalizzazione e farlo funzionare non siano andati correttamente al loro posto.

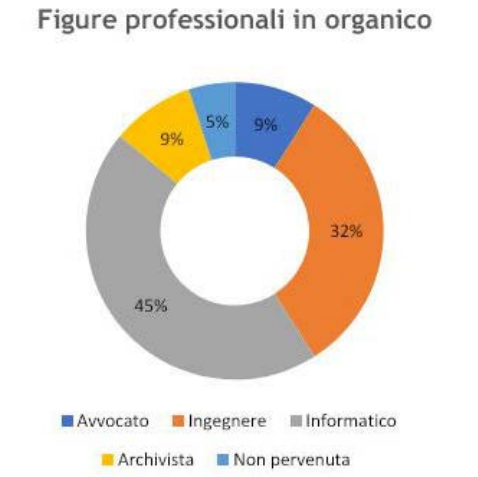
Dai dati emerge come **solo il 35% degli enti intervistati abbia nominato figure professionali ormai da tempo obbligatorie**, negli enti pubblici come in quelli privati, come il Responsabile della Conservazione, il Responsabile della gestione documentale e il Responsabile del trattamento dei dati, mentre solo il 27% degli enti ha formalizzato la nomina del *Chief Digital Officer* (CDO), figura corrispondente al Responsabile della transizione digitale previsto dall'articolo 17 del Cad (Codice dell'amministrazione digitale)[2]**. Anche dal punto di vista delle competenze i dati raccolti hanno messo in luce uno squilibrio**, segnalando la netta predominanza nel personale della PA di ingegneri e informatici, privilegiando quindi competenze prevalentemente tecniche a scapito delle competenze archivistiche e giuridiche, che pure sono fondamentali per una gestione digitale oculata dell'intero ciclo documentale: la multidisciplinarità è infatti uno dei principi che dovrebbe essere alla base dell'organizzazione interna di ogni ente.

Quanto emerso da questa "istantanea" della situazione di alcune delle più rappresentative PA centrali del nostro Paese è oggetto di indagine anche da parte della Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle pubbliche amministrazioni, guidata dall'on. Coppola, che sta facendo ulteriore chiarezza sul mancato rispetto, da parte dei principali enti pubblici italiani, della normativa sulla digitalizzazione, trasgressione verso la quale c'è stata finora una diffusa tolleranza che ha portato alla mancata applicazione delle sanzioni previste.

Eppure le leggi di riferimento ci sono, basterebbe attuarle, come **ha ribadito di recente l'Avv. Andrea Lisi** – Presidente di ANORC Professioni.

Intanto, dopo la parentesi di questa significativa indagine, il Gruppo di Lavoro delle PA Centrali avviato da ANORC e ANORC Professioni continua la sua attività, con l'intento di definire a breve un "metamodello" di governance digitale dei dati e documenti attuabile in ogni amministrazione italiana, una infrastruttura costituita da norme, modelli, schemi di competenze, figure professionali, regole tecniche e indicazioni operative che possa essere adattata a ogni realtà, tenendo conto anche della continua evoluzione delle tecnologie dell'informazione e della comunicazione.





Note

[1] *INAIL, INFN, INPS, MEF, ENEA, MIUR, Corte dei Conti, Consob, Banca d'Italia, Agenzia Industrie Difesa, ACI, Sogei, Istituto Poligrafico Zecca dello Stato, Unitelma Sapienza, MISE, Ministero del Lavoro, Consiglio Nazionale della Ricerca, Regione Valle d'Aosta, INDIRE, Informatica Trentina Spa, A.R.I.T., Arpa Lombardia, Società Informatica Territoriale Srl*

[2] Il report completo della rilevazione effettuata è scaricabile a questo link

Quale futuro per l'intelligenza artificiale nella Pubblica Amministrazione?

Marco Scialdone - *Avvocato esperto in diritto d'autore e delle nuove tecnologie*

Nell'ottobre 2016, l'amministrazione statunitense ha pubblicato il report *Preparing for the future of Artificial Intelligence* dedicato, in parte, **all'uso dell'intelligenza artificiale per migliorare la qualità dei servizi offerti dalle agenzie federali**.
Di particolare interesse risulta essere il riferimento al programma *Education Dominance* realizzato dalla DARPA (*Defense Advanced Research Projects Agency*, l'agenzia governativa del Dipartimento della Difesa degli Stati Uniti, incaricata dello sviluppo di nuove tecnologie per uso militare) grazie al quale, sfruttando le potenzialità dell'intelligenza artificiale, si mira a ridurre, da anni a mesi, il tempo necessario affinché le nuove reclute possano acquisire competenze tecniche.
Una prima valutazione del programma, basato sull'uso di un tutor digitale che usa l'intelligenza artificiale per modellare l'interazione tra un esperto e un novizio, ha evidenziato che i soggetti così addestrati superano frequentemente, sia nei test scritti che nella risoluzione di problemi nel mondo reale, reclute con 7-10 anni di esperienza.

Allo stesso modo, è stato riscontrato che i lavoratori che abbiano completato un **percorso formativo che utilizza un tutor digitale** come quello sopra descritto hanno maggiori probabilità di ottenere un lavoro ad alto contenuto tecnologico.
Proprio per questo la sezione in commento del report si chiude con due raccomandazioni: da un lato l'invito a esplorare tutte le modalità per migliorare la capacità delle agenzie federali di utilizzare l'intelligenza artificiale nel raggiungimento dei propri scopi istituzionali, dall'altro l'invito alle predette agenzie a lavorare insieme per sviluppare e condividere standard e *best practice* sull'uso dell'intelligenza artificiale nelle operazioni governative.
Tornando ai confini nazionali, **lo scorso 4 maggio la Camera dei Deputati ha approvato all'unanimità una mozione** con cui il Governo si è impegnato a:

a) promuovere iniziative, anche normative, volte all'istituzione di una cabina di regia a livello governativo per garantire un approccio onnicomprensivo allo **sviluppo della robotica e dell'intelligenza artificiale all'interno della pubblica amministrazione**, al fine di migliorare i servizi e le prestazioni al cittadino;
b) favorire l'introduzione di programmi su scala nazionale per **potenziare l'ecosistema tecnologico e industriale** legato alla robotica e all'intelligenza artificiale, a partire dalle scuole e dalle università;
c) rafforzare i modelli produttivi tendenti a valorizzare il ruolo della robotica e dell'intelligenza artificiale, anche sulla base del **programma governativo Industria 4.0**;
d) valutare, di concerto con quanto già disposto a livello comunitario, e in particolare dal Parlamento europeo, **l'introduzione di uno status giuridico specifico per i robot**, con particolare riferimento ai profili etici e di responsabilità civile, nonché in ambito fiscale;
e) avviare iniziative, anche normative, per **promuovere nuovi profili occupazionali legati all'innovazione tecnologica** e che compensino le possibili conseguenze dello sviluppo della robotica e dell'intelligenza artificiale sul lavoro umano.

A riprova del grande interesse che la tematica sta suscitando, si segnala altresì il **costituendo gruppo di lavoro in seno all'Agenzia per l'Italia Digitale** finalizzato a comprendere come la diffusione su larga scala dell'intelligenza artificiale possa "incidere nella costruzione di un nuovo rapporto tra Stato e cittadini e analizzare le conseguenti implicazioni sociali relative alla creazione di ulteriori possibilità di semplificazione, informazione e interazione".
Il predetto gruppo di lavoro avrà il compito di "(a) studiare e analizzare le principali applicazioni relative alla creazione di nuovi servizi al cittadino, definendo le strategie di gestione delle opportunità per la pubblica amministrazione; (b) mappare a livello italiano i principali centri - universitari e non - che operano nel settore dell'IA con riferimento all'applicazione operativa nei servizi al cittadino; (c) mappare il lavoro già avviato da alcune amministrazioni centrali e locali proponendo azioni da intraprendere per l'elaborazione di policy strategiche; (d) evidenziare e studiare le implicazioni sociali legate all'introduzione delle tecnologie di IA nei servizi pubblici".
Purtroppo, analoga attenzione al ruolo che l'intelligenza artificiale potrà assumere nel comparto pubblico non sembra ravvisarsi nel recente *Piano triennale 2017-2019 per l'informatica nella pubblica amministrazione*.
Invero, **l'intelligenza artificiale potrebbe essere d'ausilio** sia **nella gestione dei servizi e**, in particolar modo, **dei rapporti con i cittadini**, sia nella determinazione delle politiche migliori da implementare a livello locale.
Non mancano già esempi di utilizzo dei *chatbot*, come

Musei Italiani che fornisce informazioni in tempo reale sui musei di un'area geografica di interesse del richiedente, oppure quello realizzato per il Gruppo Torinese Trasporti che consente agli utenti del servizio, una volta inserito il numero della palina, di conoscere gli orari di arrivo in fermata di tram e bus ma anche avere una mappa con gli indirizzi dei rivenditori di titoli di viaggio più vicini.
Interessante, poi, il caso del comune siracusano di Solarino, che utilizza l'intelligenza artificiale per agevolare il rapporto tra cittadino e pubblica amministrazione: il sistema fornisce informazioni o assistenza al cittadino, inclusa la possibilità di richiedere un documento da ritirare poi in sede, il tutto senza l'intervento umano.
Come si accennava poco sopra, **l'intelligenza artificiale** è destinata ad avere un ruolo importate anche per ciò che concerne **la previsione degli effetti delle decisioni che le Pubbliche Amministrazioni intendono adottare**.

Come ricorda Alessio Plebe, Professore Associato presso il Dipartimento di Scienze Cognitive dell'Università di Messina, "dal 2008, il gruppo diretto da Tom van Engers dall'Università di Amsterdam sta personalizzando agenti artificiali ad interpretare ruoli specifici di interesse per simulare l'effetto di scelte legislative del governo olandese, in materia di riscossione tasse e di servizi all'immigrazione. Esistono diversi modelli di agenti orientati alla gestione pubblica di emergenze come alluvioni, incendi, frane, terremoti, come D4S2 (*Dynamic Discrete Disaster Decision Simulation System*) sviluppato all'università di Pittsburgh".
Siamo in presenza, dunque, di una rivoluzione, tanto nel modo di rapportarci con le pubbliche amministrazioni, quanto nel modo stesso di concepire le politiche pubbliche.
Una rivoluzione più vicina di quanto si possa pensare: del resto, per citare il poeta William Blake, "quello che oggi è dimostrato fu un tempo solo immaginato".

UNITELMA SAPIENZA

EDITORE

CLIOEDU

PARTNERSHIP SCIENTIFICA

Digital & Law Department

CON IL PATROCINIO DI

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ANORC ANORC Professioni

DIVENTA UN PROFESSIONISTA DELLA GOVERNANCE DIGITALE

MASTER UNIVERSITARIO DI 1° LIVELLO

I PROFESSIONISTI DELLA DIGITALIZZAZIONE DOCUMENTALE E DELLA PRIVACY

01. DIDATTICA INTERAMENTE ON-LINE

02. ACCESSO ALLE LEZIONI SENZA VINCOLI DI LUOGO E ORARI

03. DOCENTI DI ALTO PROFILO SCIENTIFICO

Programma del Master, informazioni e iscrizioni su www.mastergovernancedigitale.eu

Il Master fa parte dell'offerta formativa dell'Università telematica UNITELMA SAPIENZA e riconosce 60 Crediti Formativi Universitari

Obiettivi. Il Master "I professionisti della digitalizzazione documentale e della privacy" fornisce una preparazione manageriale completa e multidisciplinare con la quale affrontare e risolvere le sfide poste dalla progressiva digitalizzazione degli enti, sia pubblici che privati.

Attraverso un programma multifocale che non trascura alcun aspetto, comprendendo quello giuridico, informatico, economico e comunicativo, i partecipanti acquisiranno le competenze necessarie a sfruttare tutti i vantaggi dell'innovazione e dei nuovi processi da essa attivati, gestendo correttamente questo cambiamento che, se governato nel modo giusto, porterà innegabili miglioramenti nell'attività di ogni organizzazione, permettendo un taglio e una razionalizzazione dei costi oltre che la possibilità di offrire all'utente un servizio sempre più immediato e di più alto livello.

Le competenze che il Master mira a sviluppare sono in linea con quelle previste dallo European e-Competence Framework (e-CF), che delinea 40 competenze richieste e praticate nel contesto lavorativo dell'Information and Communication Technology a livello europeo.

Il Master, inoltre, rappresenta uno dei percorsi di riferimento nel panorama nazionale per formare **professionisti con conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati** (i cosiddetti **DPO** - Data Protection Officer), figure che sono previste come obbligatorie per gli enti pubblici e le Pubbliche Amministrazioni - e in altri specifici casi previsti dalla nuova normativa UE - a partire dal mese di maggio del 2018.

Direzione del Master

AVV. ANDREA LISI

Avvocato esperto in diritto dell'informatica e delle nuove tecnologie

Coordinamento scientifico

PROF. DONATO A. LIMONE

Ordinario di Informatica Giuridica e docente di Scienza dell'Amministrazione digitale, Direttore del Dipartimento di Scienze giuridiche ed economiche Università degli Studi di Roma Unitelma Sapienza

CONVENZIONE
CLIOEDU - ANORC

SCONTO RISERVATO AI SOCI ANORC SUL COSTO DI ISCRIZIONE

ANORC

info@mastergovernancedigitale.eu

La strategia digitale italiana: eGovernance o eGovernment

Alessandro Selam - *Direttore generale ANORC - ANORC Professioni - AIFAG*

E anche quest'anno, come ogni anno, è giunta l'estate e con la stessa puntualità è **arrivata la Relazione della Commissione Europea sui progressi in ambito digitale degli Stati membri**[1].
La Relazione, anche se fa registrare alcuni miglioramenti tra i dati rilevati nel 2015 e i dati del 2016, non è certo confortante. In questa classifica, che indirettamente valuta la modernità, **l'Italia, infatti, invece di essere tra i "big"** - come converrebbe a uno dei Paesi fondatori della Comunità europea - **si attesta nella seconda colonna della classifica** (volendo utilizzare un paragone calcistico) **e neppure in buona posizione**.
Tra gli elementi presi in considerazione dalla Relazione, genera maggiore sconforto quello legato alle competenze digitali: siamo terzultimi.
Ma non dobbiamo abbatterci, una buona notizia (per chi riesce a conservare uno spirito positivo) c'è: possiamo solamente migliorare rispetto a quanto fatto nel 2016 e, a quanto si legge sulla stampa, pare siamo sulla buona strada.
Abbiamo iniziato a porre in essere un approccio sistemico, pianificando per gli anni a venire una strategia per lo sviluppo delle competenze digitali.
Questo nuovo atto di pianificazione pluriennale si aggiunge ai numerosi atti sulla digitalizzazione (o, come viene chiamata oggi "la trasformazione digitale") che per oltre un decennio e con differente efficacia si sono stratificati sia a livello comunitario che e a livello nazionale. A livello nazionale il nostro Paese ha elaborato una propria strategia (Agenda Digitale Italiana e Piano triennale dell'informatica nella pubblica amministrazione 2017 – 2019), individuando priorità, modalità di intervento e obiettivi, che prevedono il pieno coinvolgimento delle pubbliche amministrazioni.
Il punto che emerge come necessario è quello relativo al capitale umano. **Individuare le competenze necessarie alla trasformazione digitale del nostro Paese potrebbe essere, infatti, l'elemento di svolta** per approcciare in modo corretto e consapevole anche lo sviluppo degli altri asset strategici, come ad esempio i servizi pubblici digitali, la ricerca e lo sviluppo, l'integrazione della tecnologia digitale e l'utilizzo di Internet.
La digitalizzazione non può essere a costo zero ma soprattutto non può attuarsi senza un cambiamento culturale e sociologico dei processi, e in questo lo Stato dovrebbe dare un segnale forte, abbandonando l'idea di poter costruire una solida politica di sviluppo digitale senza investire (anche economicamente) per lo sviluppo di competenze e nuove figure professionali.
Digitalizzando la pubblica amministrazione nel lungo periodo si potrebbero ottenere diversi vantaggi, non solo in termini di spesa (grazie alla semplificazione dei processi), ma anche sul piano culturale, portando tutti i soggetti coinvolti a un livello elevato di alfabetizzazione digitale.
L'impegno è davvero gravoso ma ormai improcrastinabile.
Il Legislatore ha già da tempo dettato lo scadenziario degli adempimenti in tema di digitalizzazione e i termini sono già scaduti infruttuosamente.
Non si tratta solo di gestire le competenze tecnico-informatiche dei circa 42.000 dipendenti che operano nell'ICT pubblica (circa 18.000 nelle Pubbliche amministrazioni centrali - PAC, più di 4.000 nelle società in house centrali, 14.000 nelle Pubbliche amministrazioni locali - PAL e circa 6.000 dipendenti delle società in house locali)[2], ma di **coinvolgere nel cambiamento e nella formazione anche i dipendenti pubblici non direttamente impiegati in ambito ICT**, permettendo loro di operare correttamente. Per questa ragione **sarebbe auspicabile che anche nella formulazione dei bandi per la selezione del personale si iniziassero a prendere in seria considerazione competenze adeguate e formazione specifica** per le figure individuate dal Codice dell'Amministrazione Digitale (ormai oltre un decennio fa), anziché una semplice e generica "verifica della capacità di utilizzo delle apparecchiature e delle applicazioni informatiche più diffuse (Word, Excel, Posta elettronica, Internet)"[3].
Le competenze attualmente richieste nei bandi pubblici vanno a scontrarsi con quanto previsto anche dall'Agenda digitale per l'Europa, lanciata nel maggio 2010, che ha promosso la realizzazione nell'UE di 101 azioni, strutturate in sette aree prioritarie per la crescita digitale e l'aumento del tasso occupazionale.

In tale prospettiva**, anche l'Italia ha elaborato una propria strategia nazionale, individuando priorità, modalità di intervento e obiettivi, che prevedono il coinvolgimento diretto degli enti locali**, attraverso l'individuazione delle seguenti azioni infrastrutturali trasversali:

- connettività e infrastrutture in banda ultra larga e predisposizione wi-fi presso tutti gli edifici pubblici;
- razionalizzazione del patrimonio ICT e Digital Security per la PA;
- consolidamento data center e cloud computing;
- digitalizzazione delle infrastrutture di servizi e delle piattaforme abilitanti:
  - Servizio Pubblico d'Identità Digitale (SPID)
  - piattaforme abilitanti (Anagrafe Popolazione Residente, pagamenti elettronici, fatturazione elettronica PA, Open Data, sanità digitale, scuola digitale, giu-

stizia digitale, turismo digitale, agricoltura digitale);

- digitalizzazione dei servizi di settore azienda-cittadino con la Pubblica amministrazione;
- programmi di accelerazione (Open data, Italia Login – la casa del cittadino, Smart City & Communities)
- competenze digitali.

Le azioni previste devono essere contestualizzate nel generale processo di riforma della PA, avviato dal Governo sulla base della legge delega n.124/2015, che ha condotto all'approvazione del testo di modifica del Codice dell'Amministrazione Digitale. Il Codice di riferimento per le Pubbliche Amministrazioni ha subìto un allineamento alle nuove scelte derivanti dai programmi in corso di attuazione in ambito europeo (soprattutto per identità digitale e domicilio digitale) e in tema di governance, oltre all'abrogazione di norme non attuate o obsolete.
In relazione all'evoluzione dello scenario comunitario e nazionale, **anche le Amministrazioni comunali sono chiamate a svolgere un ruolo cruciale** per la definizione di obiettivi e linee d'azione concrete in campo digitale. Nello specifico, dunque, si tratta di individuare una strategia in grado di supportare la realizzazione dell'Agenda Digitale Locale, finalizzata a promuovere la partecipazione attiva dei cittadini, incrementando il tasso di innovazione, l'efficienza e la sostenibilità del sistema degli Enti locali.
Il quadro normativo di riferimento delineatosi negli ultimi anni ha previsto, in particolare, **una serie di scadenze successive, con provvedimenti che non hanno senso se applicati in maniera distinta, ma devono essere correttamente interpretati secondo la logica predominante del "digital first"** e contestualizzati all'interno dello scadenzario complessivo, che ha lo scopo di portare alla realizzazione di validi processi documentali interamente digitali.
Lo scadenzario della digitalizzazione dei processi documentali ha inizio con un intervento nella fase corrente del ciclo di gestione, per cui le PA sono state chiamate, ancora una volta, a implementare una corretta gestione documentale informatica, riprendendo quanto già stabilito fin dal 2000 con le precedenti regole tecniche sul protocollo informatico. Le nuove regole non hanno rivoluzionato di fatto quanto già statuito in passato, ma hanno introdotto, tra gli altri, un nuovo obbligo che, se non rispettato, rischia d'invalidare gli sforzi messi in atto dalle PA per la corretta gestione del protocollo informatico: dall'11 ottobre 2015, infatti, è diventata obbligatoria la conservazione "a norma" del registro di protocollo informatico entro il giorno successivo alla sua formazione.
A livello organizzativo l'Ente si troverà ad attuare, sia sul piano verticale che su quello orizzontale le seguenti azioni:

- processo di digitalizzazione informativa e documentale;
- sviluppo delle infrastrutture per i servizi pubblici digitali;
- sviluppo delle competenze digitali;
- realizzazione di un sistema di dialogo avanzato con il cittadino, per l'erogazione e la fruizione dei servizi.

Gli interventi specifici dovranno riguardare:

- documenti amministrativi da adottare o aggiornare;
- manuale di gestione documentale;
- manuale di conservazione;
- nomine Responsabili;
- piano anticorruzione e trasparenza;
- regolamenti e documenti necessari per il corretto trattamento dei dati personali;
- sistemi di formazione, gestione e archiviazione documentale;
- creazione di documenti informatici validi: mappatura dei processi;
- verifica degli strumenti di ricezione delle istanze: semplificazione amministrativa;
- definizione dei livelli SPID;
- sistema di protocollo generale conforme alla normativa;
- sistema di gestione documentale conforme alla normativa;
- adozione della corretta soluzione di conservazione documentale.

L'adeguamento delle banche dati comporta:

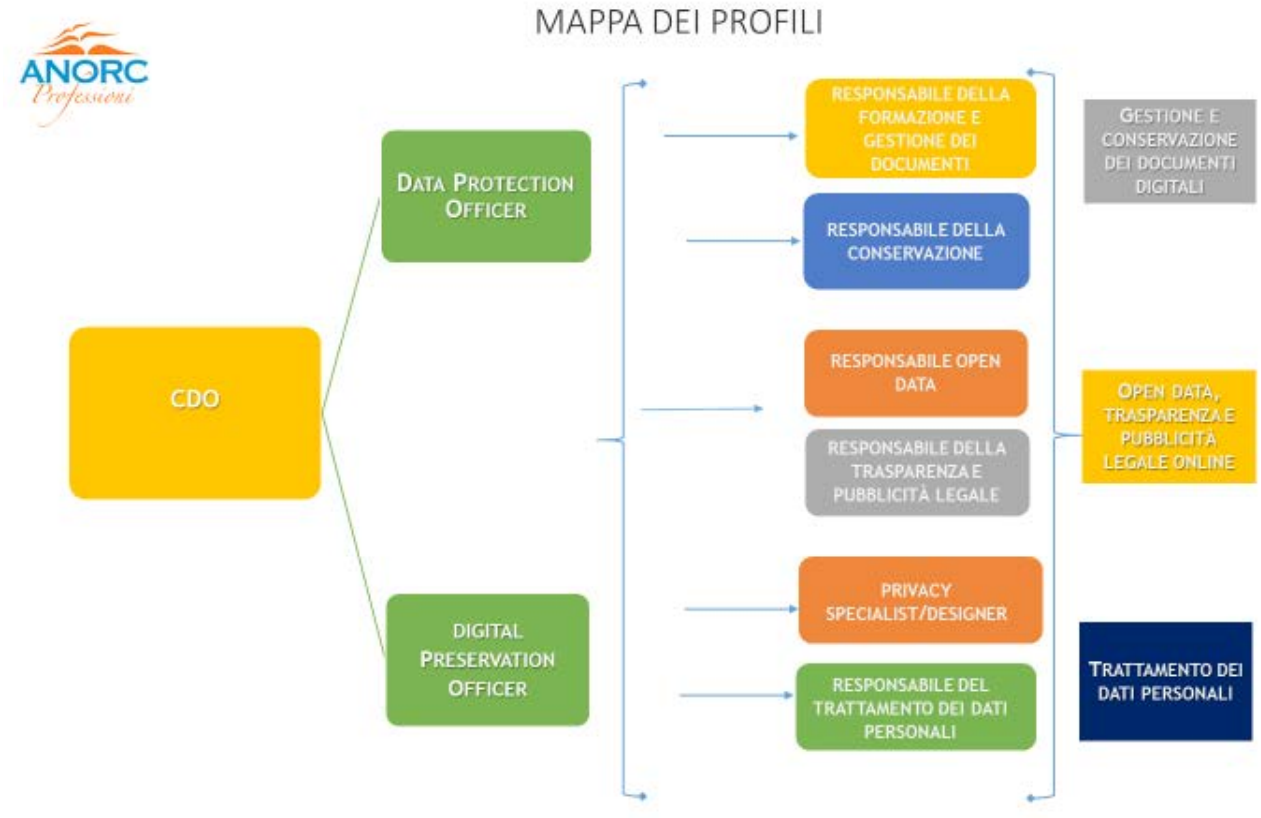
- verifica del livello di interoperabilità delle banche dati;
- adozione di soluzioni tecnologiche che consentano il dialogo in cooperazione applicativa;
- verifica delle misure di sicurezza adottate a tutela dei dati contenuti, nel rispetto della privacy;
- definizione policy per aggiornamento e pubblicazione dei dati nel rispetto della normativa sulla trasparenza.

Le figure professionali obbligatorie da nominare e formare sono:

- Manager della transizione digitale o CDO – *Chief Digital Officer* (art. 17 del CAD);
- DPO – Data Protection Officer;
- Responsabile della gestione documentale;
- Responsabile anticorruzione, trasparenza e pubblicità legale;
- Responsabile Open Data;
- Responsabile della conservazione;
- Responsabile della sicurezza informatica e dei sistemi informativi autorizzati.

Sulla base degli obblighi previsti all'interno degli enti pubblici e privati da oltre un anno, **ANORC, ANORC Professioni e numerosi Enti[4] si stanno confrontando in un gruppo di lavoro per elaborare un modello condiviso di governance per la gestione digitale dei dati e dei documenti**.
Da tale confronto, che coinvolge anche alcune rappresentanze di enti territoriali, è nato un modello che ha la caratteristica di comprendere tutte le competenze necessarie alla generazione, gestione, conservazione e protezione dei dati e delle informazioni in possesso delle PPAA (sintetizzato nello schema qui di seguito). L'elemento di novità dirompente del modello di tale governance è dato dall'aver integrato sin dall'inizio gli aspetti propri della digitalizzazione con quelli della protezione dei dati personali, recentemente uniformati a livello comunitario dal Regolamento UE 679/2016.
Per rendere più stringente la realizzazione di questi obiettivi per ciò che riguarda formazione, competenze e modelli di governance (come capisaldi sui quali sviluppare innovazione e processi di digitalizzazione reali), l'art. 12 del Codice dell'Amministrazione Digitale[5] definisce il ruolo dei decisori pubblici e della dirigenza.

Come si evince dal comma 1, per realizzare gli obiettivi viene previsto un ulteriore documento, il Piano triennale per l'informatica nella Pubblica amministrazione 2017 – 2019, pubblicato il 31 maggio scorso con lo scopo di proporre alle PA di contribuire allo sviluppo e alla crescita dell'economia del Paese attraverso l'indicazione degli strumenti che permetteranno lo snellimento dei procedimenti burocratici, la maggiore trasparenza dei processi amministrativi e una maggiore efficienza nell'erogazione dei servizi pubblici.
Il Piano propone un modello sistemico, diffuso e condiviso, di gestione delle tecnologie digitali più innovative, improntato a uno stile di management agile ed evoluto, e basato su una chiara governance dei diversi livelli della PA[6].
Al centro di questo modello bisogna prevedere una figura di vertice - così come stabilito all'articolo 17 del CAD - e allo stesso tempo bisogna lavorare affinché venga attuata non solo la governance digitale come modello organizzativo, ma anche dei processi di eGovernment reali in grado di supportare il cambiamento e l'attuazione dell'Agenda digitale.
È ormai sempre più evidente, quindi, che **per vincere questa sfida le risorse umane a disposizione della PA svolgeranno una funzione determinante**: mettere subito in atto, su tutto il territorio nazionale (enti centrali e locali), un programma di formazione e aggiornamento mirati all'acquisizione delle competenze necessarie alla gestione digitale (su più livelli di responsabilità) dei processi documentali, modificare i criteri di reclutamento del personale della PA, introdurre nuovi e funzionali schemi operativi, mettere in campo dei finanziamenti a supporto di questo cambiamento sono perciò le azioni che ci si aspetterebbe da un Governo veramente intenzionato a portare a compimento una trasformazione da cui dipende lo sviluppo (anche economico) del nostro Paese.
In attesa che si palesino fatti incoraggianti (perché non è più il tempo dei segnali da interpretare), gli stakeholders si organizzano e **per fortuna germogliano iniziative di alta formazione** come quella messa in campo dall'Università Unitelma Sapienza con la collaborazione di ANORC e ANORC Professioni: il primo Master Universitario di 1° livello caratterizzato dalla contaminazione "positiva" delle competenze e delle professionalità che si occupano di protezione dei dati personali e di digitalizzazione.
L'elemento innovativo di percorsi formativi di questo tipo risiede nell'essere appositamente progettati per formare la nuova generazione di manager che dovranno farsi carico della "transizione digitale" (come viene chiamata ora), rispondendo quindi alle reali esigenze formative che emergono per chi lavora sul campo e trattando tutti gli aspetti che chi si occupa di digitale si trova a dover governare: conoscenze normative, organizzative e applicative, tanto in materia di trattamento dei dati personali quanto di gestione e conservazione digitale di dati, documenti e informazioni.
L'augurio che possiamo farci è che in futuro si presti sempre maggiore attenzione alle reali esigenze degli operatori, siano essi pubblici o privati, cercando di dare seguito e ampia applicazione a iniziative che nascono dalla buona volontà di chi deve realmente e quotidianamente gestire la digitalizzazione.



Note

[1] Sul sito della Commissione Europea è possibile visionare il Report per intero oppure le rilevazioni per ciascuna singola categoria presa in esame https://ec.europa.eu/digital-single-market/en/european-digital-progress-report.

[2] Fonte dei dati: Piano triennale dell'informatica nella pubblica amministrazione 2017 – 2019.

[3] Tra i moltissimi casi si consideri il recente bando pubblicato dal Comune di Firenze: http://www.comune.fi.it/materiali/concorsi/CP/IDA-2017-Bando.pdf.

[4] Agenzia Industrie Difesa, Agenzia Industria Spaziale, Agenzia Regionale per l'Informatica e la Telematica, ARPA Lombardia, Automobile Club d'Italia, Banca d'Italia, Consiglio Nazionale della Ricerca, Consob, Corte dei Conti, ENEA, Informatica Trentina S.p.A., InnovaPuglia S.p.A., Insiel S.p.A., Istituto Nazionale Analisi Politiche Pubbliche, Istituto Nazionale Assicurazione Infortuni sul Lavoro, Istituto Nazionale Documentazione Innovazione Ricerca Educativa, Istituto Nazionale Fisica Nucleare, Istituto Nazionale Previdenza Sociale, Istituto Nazionale di Statistica, Istituto Poligrafico Zecca dello Stato, LAZIOCrea S.p.A., Ministero dell'Economia e delle Finanze, Ministero dell'Istruzione dell'Università e della Ricerca, Ministero del Lavoro, Ministero dello Sviluppo Economico, Società Informatica Territoriale S.r.l., Sogei S.p.A., Regione Friuli Venezia Giulia, Regione Sicilia, Regione Toscana, Regione Valle d'Aosta, Umbria Digitale S.p.A., Università Unitelma Sapienza.

[5] D.Lgs. 82/2005, art. 12: "1. 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 previsti dal CAD in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui all'articolo 14-bis, comma 2, lettera b).

1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150, dettano disposizioni per l'attuazione delle disposizioni del CAD.

1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al (presente Codice) ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del CAD è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti."

[6] https://pianotriennale-ict.italia.it/

Know IT è la piattaforma di formazione e informazione dedicata ai professionisti dell'era digitale. Il percorso di digitalizzazione, anche se a piccoli passi, sta rivoluzionando gli scenari di mercato, aprendo nuove prospettive e nuove criticità per la privacy, il commercio elettronico, il diritto d'autore e la conversione in digitale di processi prima analogici, come la fatturazione, la gestione documentale, la firma. Tutto ciò avrà un impatto sempre maggiore su molti aspetti organizzativi, coinvolgendo PA, aziende, professionisti e cittadini.

Know IT si propone di diffondere una conoscenza digitale che si allarghi dall'area prettamente tecnica a quella normativa e gestionale, implementando la capacità degli utenti di valutare e condurre i nuovi processi e modelli organizzativi, ottimizzandoli e fornendo valore aggiunto al contesto in cui si trovano a operare.

Il nostro programma formativo affronta in particolare le seguenti macrotematiche: e-commerce, diritto d'autore, privacy e sicurezza, firme elettroniche e biometria, e-government, e-health, document management e, in generale, tutti i principali aspetti dell'ICT law.

Corsi on demand dedicati a PA, aziende e professionisti

SCOPRI L'OFFERTA FORMATIVA

www.knowit.clioedu.it

Digital & Law Department
www.studiolegalelisi.it

CLIOEDU®