



Speciale DIG.Eat 2019

Lato B

Direzione Scientifica: Andrea Lisi

Limited Edition

Speciale DIG.Eat 2019

Evento organizzato da: ANORC
Con il supporto di: Digital&Law Department

Curatrice Editoriale: Francesca Cafiero

Edizioni Moscara Associati
Progetto grafico e impaginazione:
Studio Moscara Associati Progetti d'Autore
www.moscara.it

I titoli degli articoli presenti nella rivista sono liberamente
ispirati alla discografia dei Pink Floyd

the dark side of...





con il patrocinio del
Ministero della Salute



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**





F R E E

FOUR

Una riflessione sulla stagione di lavori appena conclusa



F R E E

FOUR

di Alessandro Selam, direttore di ANORC

In occasione del DIG.Eat 2019 Alessandro Selam affronta il lato oscuro dell'azione associativa, presentando gli esiti della Stagione di lavori 2018/19 di ANORC, appena conclusa. Il direttore riflette sull'importanza di trovare uno spazio di dialogo associativo, rinnovando l'impegno di proseguire il confronto in previsione dell'apertura della nuova stagione di attività.

Uno spazio di confronto e di dialogo. È quello che ANORC ha inteso realizzare nel corso dell'ultima stagione di lavori 2018/19, con la creazione di quattro tavoli di lavoro dedicati rispettivamente a quattro macro-tematiche di grande attualità: **Firme e sigilli elettronici, Fatturazione elettronica, Conservazione in-house per le PA e GDPR, sistemi e processi di conservazione.**

La selezione dei temi di dibattito è stata condotta dagli stessi associati aderenti all'iniziativa, interessati a sviluppare un confronto utile a evidenziare le criticità nell'applicazione della normativa vigente in ciascuno dei rispettivi settori, contribuendo ad individuare possibili soluzioni, lato impresa.

La scelta di **presentare i risultati dei lavori alla XII edizione del DIG.Eat** assume particolare significato per la nostra realtà associativa che, attraverso la condivisione di quanto svolto in questi mesi, intende procedere verso **l'inaugurazione della nuova stagione di lavori 2019/20**, all'insegna della partecipazione e della proattività.

Procedendo con ordine, i risultati di questa stagione sono così sintetizzabili: il confronto sulle firme e sigilli elettronici, **coordinato dall'ing. Giovanni Manca**, ha avuto quale esito un complesso elaborato che analizza i sistemi di firma, di sigillo e di identità digitali e le loro applicazioni.

Il gruppo dedicato al presidio della protezione dei dati personali, **coordinato dal**

dott. Franco Cardin, ha portato avanti un progetto per l'elaborazione di un Codice di condotta all'interno dei sistemi di conservazione ex art. 40 del Regolamento UE 679/2016.

Il dialogo tra le imprese aderenti al tavolo dedicato alla Fatturazione elettronica, coordinato dall'ing. Andrea Caccia, ha consentito di condividere esperienze tra operatori coinvolti a vario titolo nel processo di fatturazione, analizzare dubbi e perplessità e proporre risoluzioni. La puntualità delle indicazioni dei partecipanti ha alimentato un confronto costante con l'Agenzia delle Entrate per il raggiungimento dell'interesse comune in un sistema aderente alle aspettative di imprese, professionisti e cittadini.

Il tavolo degli interessati alla conservazione in house, coordinato dalla dott.ssa Laura Flora, ha voluto approfondire, tra gli altri, gli argomenti della definizione dei responsabili e delle responsabilità legati alla formazione, gestione e conservazione del documento amministrativo informatico e delle possibili configurazioni del servizio di conservazione (*dal full in-house al full outsourcing*) con evidenza dei pro e dei contro di ciascuna modalità.

Alla luce di questa panoramica, è possibile individuare un denominatore comune tra le attività condotte in questa stagione, ossia l'esigenza manifestata da parte delle imprese di trovare uno spazio di confronto sull'aggiornamento e l'estensione della normativa (anche tecnica) relativa alla transizione digitale del nostro Paese.

Per rispondere a questa urgenza, riteniamo la presentazione al DIG.Eat XII delle riflessioni emerse nel corso dei lavori possa rappresentare un importante momento di crescita e maturazione per la nostra realtà associativa, anche nella prospettiva di instaurare un dialogo costante con le istituzioni di riferimento.

Attendiamo di inaugurare la nuova Stagione 2019/20

ON THE RUN

ON THE RUN

Le amministrazioni pubbliche in fuga



di Laura Flora, Istituto nazionale di astrofisica
Osservatorio astronomico di Trieste
Coordinatrice del Tavolo di Lavoro ANORC
"Conservazione in house per le PA"

In occasione del DIG.Eat 2019 Laura Flora affronta il lato oscuro dell'amministrazione digitale. L'Amministrazione pubblica deve riuscire a stare al passo con i tempi, adattandosi e modificandosi rapidamente, per rispondere in modo adeguato ai bisogni dell'utenza e al miglioramento dei servizi interni. Il trucco? Cambiare l'approccio strategico.

Tradendo un chiaro riferimento generazionale, *"The dark side of"* non può che evocare un riferimento musicale miliare; ed è proprio cogliendo questo spunto che voglio riferirmi a uno dei brani contenuti nell'"album" storico dei Pink Floyd *"The dark side of the moon"*, per inviare il messaggio sulla PA che vorremmo: *On the run - In fuga*.

E' questa la PA che ci piacerebbe disegnare: giovane, dinamica, al passo con i tempi e con le nuove tecnologie.

Nel tempo in cui si usano sempre più i messaggi vocali, o, al limite, la funzione di dettatura vocale, e sempre meno lo scritto, l'Amministrazione pubblica "fit" deve riuscire a stare al passo con i tempi, adattandosi e modificandosi rapidamente, solo così potrà rispondere in modo adeguato ai bisogni dell'utenza e al miglioramento dei servizi interni.

Strategico deve essere l'approccio, culturale, strategiche devono essere le nuove figure che si occupano dell'amministrazione pubblica già digitale, perché è la società ad essere già velocemente digitale.

La sfida

Anche l'approccio alla conservazione digitale, così come la scelta delle **possibili configurazioni del servizio di conservazione se full in-house o full outsourcing**, non può ridursi a un mero aspetto tecnologico. Allo stato il problema e l'impostazione normativa sono molto legati all'aspetto informatico e meno mirati all'aspetto organizzativo-gestionale: prima di scegliere come conservare dobbiamo capire cosa conservare e per quanto tempo. Fino ad ora la normativa ha dato indicazioni "a macchia di leopardo" ragionando per tipologie documentarie o per serie (le fatture elettroniche, il registro di protocollo informatico) senza calare tutto ciò in un coerente quadro d'insieme. Ebbene, la svolta strategica deve essere questa. Bisogna ragionare sulla memoria digitale senza perdere di vista la visione globale e il legame documentale, il "vincolo archivistico", focalizzando l'attenzione sul fascicolo. E' evidente che la valutazione in house o in outsourcing non può che presupporre la necessaria valutazione di costi/benefici. La digitalizzazione è fondamentale: ma ciò che il prodotto gestionale deve consentire di mandare in conservazione in modo facile e user friendly è il fascicolo. Cominciamo a ragionare di fascicoli o di serie documentarie e definiamo, coerentemente, le tipologie documentarie che, incontrovertibilmente, hanno un impatto ai fini della "memoria" dell'Ente: serie come ad esempio delibere, determinazioni, dovranno essere sicuramente oggetto di conservazione permanente. Successivamente si faranno valutazioni di opportunità. Serve una opportuna e generale politica conservativa, con indicazioni normative delle tipologie da conservare, che ragionino sul fascicolo (o serie) e non su singoli documenti.

Oltre a ciò è fondamentale una revisione dei **ruoli nella PA digitale**. In realtà il problema trascende il mero ambito di gestione dei documenti ed anche dei processi per assumere rilievo in tutto il contesto operativo. Il nuovo *manager* pubblico deve organizzare diversamente il proprio lavoro ed il capitale umano che deve coordinare. E' da qui che parte l'Amministrazione in fuga, la sfida nasce dall'alto: lavorare con il proprio personale non in sede perché in telelavoro o in *smart working* disorienta, lavorare su obiettivi e performance non è facile, motivare i collaboratori sfiduciati, rispondere ad un'utenza talvolta esacerbata

richiede molto più che competenze tecniche o giuridiche o di *record manager*, richiede il perseguimento della *mission* istituzionale mantenendo l'aspetto umano-empatico e la visione d'insieme, per poter reingegnerizzare e semplificare processi e procedimenti, adattandosi: ai nuovi vincoli normativi, ad uno scarso turn over, ad agire in un contesto in cui le risorse umane non sono sempre duttili e inclini al cambiamento, alla continua evoluzione delle nuove tecnologie. Il ruolo strategico in questa sfida è proprio quello del *manager* pubblico.

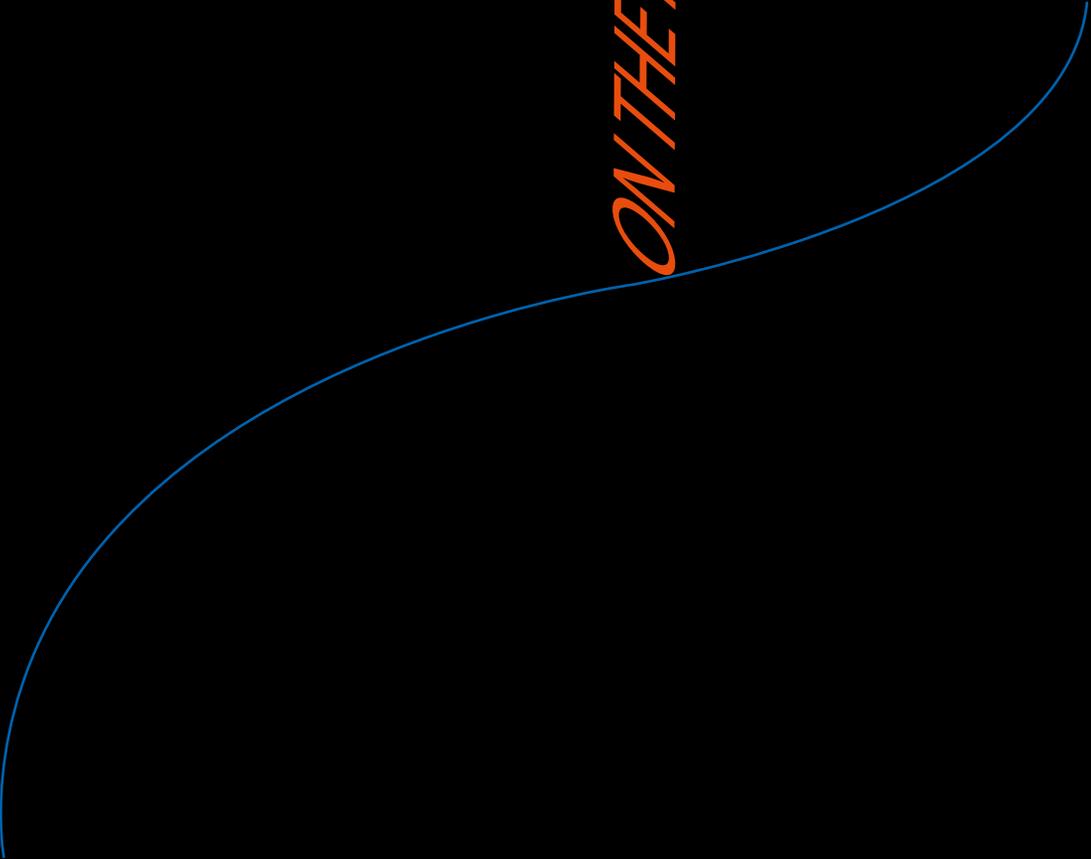
La PA che vince

La PA che vince è quella che ha al proprio interno un *team-leader* consapevole del proprio ruolo, disposto a mettersi in gioco e a imparare dai propri collaboratori e che riesce a fare gioco di squadra: ma assai oculata deve essere la scelta di questa "squadra". Che oramai sia più importante sapere cosa sia il Cloud anziché l'accessione invertita deve averlo capito anche il nostro legislatore, se si è deciso ad investire risorse per reclutare professionalità con competenze in materia di digitalizzazione, razionalizzazione e semplificazione dei processi e dei procedimenti amministrativi (ma anche, si badi, di tecnica di redazione degli atti normativi e analisi e verifica di impatto della regolamentazione). E' evidente che, attualmente, la definizione dei responsabili e delle responsabilità legati alla formazione, gestione e conservazione del documento amministrativo informatico - ciò a dire chi ricopre il ruolo di responsabile della gestione documentale e di responsabile della conservazione - sconta, per provenienza professionale ed estrazione manageriale, una scarsa reale preparazione sui temi digitali. Ed è chiaro che essendo le professionalità richiamate molteplici, richiedendosi competenze manageriali, giuridiche, archivistiche, non sia facile rinvenire chi ha competenze multidisciplinari. Ma è bene che il focus si sposti dall'aspetto prettamente informatico a quello digitale-organizzativo: la PA che vince avrà un responsabile della gestione documentale che oltre a conoscere le regole base in materia di classificazione e fascicolazione, conosce i flussi procedurali perché conosce le procedure e i processi del proprio Ente e si raccorda con il responsabile della conservazione che è stato coinvolto nelle scelte strategiche fondamentali già in fase di creazione del documento. Ed entrambi si devono coordinare con il re-

sponsabile per la transizione al digitale ed il Responsabile per la protezione dei dati. La sfida si vince così: con la "squadra" e con un team leader che è pronto a rischiare e ad ascoltare.

Questa è la PA in fuga, questa è la memoria che vogliamo conservare.

ON THE RUN *ON THE RUN*



A PILLOW OF WIND



Il futuro di firma e sigillo elettronico in Italia ed Europa.



di Giovanni Manca,

Ingegnere e Vicepresidente di ANORC
Coordinatore del Tavolo di Lavoro ANORC
"Firme e Sigilli"

In occasione del DIG.Eat 2019 Giovanni Manca affronta il lato oscuro della sottoscrizione digitale, ripercorrendone l'evoluzione normativa. Dopo 20 anni dall'adozione delle prime regole tecniche sulla firma, è giunto il momento di valutare a che punto siamo arrivati. L'identità digitale e la blockchain saranno nel futuro della firma?

Introduzione

Se il successo di una fattispecie giuridica è determinato dalla diffusione e dal livello di utilizzo, la firma digitale è sicuramente un grande successo.

Le prime regole tecniche sono nel DPCM 8 febbraio 1999, quindi la firma digitale è utilizzata da oltre vent'anni.

Nel 2019 la sottoscrizione qualificata ha raggiunto una diffusione elevatissima con oltre 21.000.000 di certificati qualificati di sottoscrizione, dei quali circa l'85% è installato per applicazioni di firma remota; questa tipologia di sottoscrizione è stata utilizzata sopra il miliardo di volte. Anche le marche temporali rilasciate hanno raggiunto e superato ampiamente un paio di miliardi. Più recente e meno diffuso l'utilizzo del sigillo qualificato.

La FEA realizzata con tecnologia grafometrica ha raggiunto decine di migliaia di postazioni, anche in mobilità, nel mondo assicurativo, bancario e industriale.

Con il regolamento europeo 910/2014 eIDAS è stata introdotta la fattispecie del sigillo elettronico. Nella sua forma qualificata è ancora poco diffuso, ma pian piano sta crescendo.

Si sta regolamentando la sottoscrizione basata sull'identità digitale e nella Leg-

ge di semplificazione 2019 si stabiliscono forma scritta e validazione temporale basate su tecnologie blockchain.

Nel mondo virtuale della Rete per quanto tempo avrà ancora senso la sottoscrizione? E quando, invece, sarà sostituita da altri strumenti?

La sottoscrizione digitale

La sottoscrizione digitale nasce come sostituto della firma autografa per i documenti digitali. La sua diffusione è stata inizialmente indotta da alcuni obblighi normativi. Con la semplificazione e l'efficienza attuate con la firma remota (l'85% dei certificati di sottoscrizione è utilizzata così) sono cresciuti moltissimo diffusione e utilizzo, fino al raggiungimento dei numeri che abbiamo mostrato in precedenza.

L'ultima ondata di crescita è stata stimolata dalla fatturazione elettronica tra soggetti privati. Il mercato non aveva l'obbligo di firmare queste fatture, ma la stessa Agenzia delle Entrate ne ha suggerito l'utilizzo per avere certezza della loro integrità e imputabilità.

Pure la firma grafometrica è molto diffusa con decine di migliaia di dispositivi installati e tante sottoscrizioni generate in scenari dove l'utente è "poco tecnologico". Peraltro, assicurazioni, banche, uffici postali e alcuni settori industriali utilizzano in modo ampio e costante la grafometrica, anche se non si dispone di statistiche di utilizzo.

Concludendo questa riflessione sulle sottoscrizioni possiamo dire che queste avranno lunga vita fino a quando i procedimenti amministrativi digitali saranno simili a quelli cartacei. Inoltre, il digitale, pur essendo in costante crescita anche nel privato è ancora poco utilizzato nella piccola e media impresa.

Il sigillo elettronico

Questo strumento è stato introdotto in eIDAS in forte analogia con la firma elettronica con la quale condivide definizione e scopo operativo finale. La firma serve per firmare (questo c'è scritto), il sigillo per garantire l'origine e l'integrità dei dati.

Normalmente e di impulso viene subito da dire che il sigillo elettronico è la fir-

ma della persona giuridica, ma un'analisi leggermente più approfondita porta a valutare che firma e sigillo non sono funzionalmente del tutto equivalenti. ANORC ha insediato un Gruppo di lavoro sul tema specifico. In tale sede si è giunti alla conclusione che il sigillo elettronico qualificato per la sua natura giuridica può sostituire in molti contesti la sottoscrizione. I contesti sono quelli dove non è importante avere certezza dell'identità del firmatario, ma della provenienza e dell'integrità del dato.

Il titolare del sigillo è una persona giuridica, quindi il numero di certificati qualificati di sottoscrizione potrebbe ridursi a favore di quelli per i sigilli.

Identità, sottoscrizione e blockchain

L'articolo 20, comma 1-bis del CAD ha introdotto una nuova fattispecie di formazione del documento informatico. Questa è legata all'identità dell'autore del documento quindi si gettano le basi per lo sviluppo del rapporto tra le identità digitali gestite con SPID (Sistema Pubblico di Identità Digitale) e la Carta d'Identità Elettronica (CIE) tenendo in conto anche il loro status di valido schema europeo di autenticazione elettronica. Al momento della scrittura di queste righe è imminente la consultazione pubblica delle Linee guida per la cosiddetta "firma con SPID". La possibilità di firmare o sigillare con le credenziali SPID ovvero con la CIE potrebbe ridurre la richiesta degli attuali certificati qualificati di sottoscrizione.

Il Legislatore nazionale ha stabilito una nuova efficacia giuridica della forma scritta mediante i registri distribuiti e gli smart contract che fanno parte del mondo della blockchain. Quindi anche questa tecnologia, in varie declinazioni, comincia a occupare spazi nelle questioni dell'identità, dell'integrità e imputabilità delle transazioni e dei documenti e della validazione temporale.

Non è ancora ben definito lo scenario di utilizzo di questi strumenti al di là del loro valore legale. Certamente sono in campo strumenti alternativi alla firma, per come la conosciamo fino ad ora.

Le tematiche che rimangono in discussione sono l'individuazione di procedi-

menti applicativi nati per il digitale e quindi non “clonati” dal mondo cartaceo e la circostanza che l’innovazione non dovrebbe essere preceduta dalla compliance normativa. Questa ne limita l’evoluzione in un periodo storico nel quale è inevitabile che la tecnologia muti a una velocità tale che il Legislatore non può seguire.

A PILLLOW
OF WIND

MOTHER MOTHER

Fattura elettronica:
da FatturaPA al nuovo standard europeo,
ecco le opportunità

MOTHER



di Andrea Caccia, ingegnere
Esperto di fatturazione elettronica
Coordinatore del tavolo di lavoro
di ANORC "Fatturazione Elettronica"

In occasione del DIG.Eat 2019 Andrea Caccia, affronta il lato oscuro della fatturazione elettronica, obbligatoria dal 1° gennaio 2019, che ha già consentito un notevole recupero di gettito. Tuttavia, i tempi molto stretti hanno reso il provvedimento più un adempimento che un'opportunità. Il nuovo standard europeo, che SDI gestisce dal 18 aprile, potrebbe essere l'occasione per un'evoluzione di FatturaPA più vicina alle esigenze del mercato

Come previsto dalla legge di bilancio 2018 dal 1° gennaio 2019 la fatturazione elettronica è diventata obbligatoria anche per il settore privato. In poco più di un anno, l'Agenzia delle Entrate, con il proprio partner tecnologico Sogei, ha adeguato ed esteso il Sistema di interscambio secondo le nuove esigenze. Il sistema è partito senza grossi problemi ed è ormai prossimo ad aver gestito mezzo miliardo di fatture. In base ai dati forniti dalla stessa Agenzia, nei primi 2 mesi del 2019 ha consentito di intercettare acquisti fittizi per 3,2 miliardi di euro corrispondenti a 622 milioni di euro di falsi crediti IVA che sono stati bloccati. La fatturazione elettronica si conferma dunque uno strumento utile a ridurre le frodi IVA e consentirà di mantenere o forse superare la previsione di maggiori entrate nel bilancio dello Stato.

Tutto bene dunque?

La risposta è negativa. Per riuscire a gestire un progetto così ambizioso ed in tempi così ristretti si è perso di vista, fino ad oggi, l'obiettivo più interessante del progetto FatturaPA originale, quello di spingere le imprese a adottare la fatturazione elettronica come stimolo per progetti di digitalizzazione dei propri processi, cogliendo così importanti benefici e andando ben oltre la logica dell'adempimento finalizzato solo

allo scopo di ridurre le frodi e il recupero di gettito.

La Direttiva (UE) 55/2014, la sua attuazione in Italia e il tavolo AgID

L'obbligo viene introdotto in Italia dal comma 1 dell'articolo 3 del citato d.lgs. 148/2018, che ricalca quanto specificato nella direttiva. Nel comma 2 viene introdotto un ulteriore requisito: si richiede la conformità alle "Core Invoice Usage Specification" (CIUS) che devono essere pubblicate mediante un provvedimento del direttore dell'Agenzia delle entrate (previsto al comma 3 e richiamato dall'articolo 5 come vedremo tra poco) che integra quanto previsto dal Decreto Ministeriale 55 del 3 aprile 2013. La possibilità di introdurre questo specifico requisito è in realtà una questione controversa in quanto la direttiva 55 non consente di introdurre requisiti nazionali aggiuntivi, a garanzia dell'interoperabilità.

L'articolo 4 dispone la deroga al 18 aprile 2020 dell'obbligo per le PA sub-centrali, l'Italia approfitta pertanto di questa possibilità concessa dalla direttiva.

Molto interessante l'articolo 5 del decreto che, a seguito del parere della Conferenza unificata e – in particolare – delle regioni, istituisce presso l'AgID il "Tavolo tecnico permanente per la fatturazione elettronica" con le seguenti funzioni:

- a) aggiornamento delle regole tecniche e delle modalità applicative di cui al comma 3 dell'articolo 3;
- b) monitoraggio della corretta applicazione delle stesse;
- c) valutazioni degli impatti per la pubblica amministrazione e di quelli riflessi per gli operatori economici;
- d) raccordo e coinvolgimento, fin dalla fase di definizione, di tutte le iniziative legislative ed applicative in materia di fatturazione e appalti elettronici.

Molto opportuno a parere di chi scrive è il coinvolgimento dell'AgID e dei rappresentanti di regioni e PA locali, che andrebbe anzi esteso a tutti i portatori di interesse, ad esempio tramite il Forum italiano sulla fatturazione elettronica. Sarebbe inoltre fondamentale l'estensione anche alla fatturazione tra privati dove l'uso di formati standard esplicherebbe i massimi benefici di sistema. Se infatti, considerati i tempi estremamente ristretti, necessari per centrare gli obiettivi di gettito, finora l'Agenzia delle entrate ha avuto carta bianca sull'introduzione dell'obbligo di fatturazione elettronica, è ora fondamentale, per il successo del progetto ed il pieno sfruttamen-

to dei benefici che può portare la fatturazione elettronica e la digitalizzazione in genere di processi, che siano coinvolti tutti gli attori. L'articolo 4 va in questa direzione richiedendo per la prima volta che siano valutati gli impatti riflessi per gli operatori economici e, col punto d), mettendo il tavolo al centro di tutte le iniziative future. Da notare anche la possibilità di utilizzare lo standard europeo per le fatture domestiche che, per quanto già discusso, è un'opportunità molto interessante. Si noti quanto previsto dal considerando 4 della direttiva: "la Commissione e gli Stati membri dovrebbero adoperarsi affinché i costi a carico degli utenti della norma europea sulla fatturazione elettronica, in particolare microimprese, piccole e medie imprese, siano ridotti al minimo in modo da facilitarne la diffusione in tutta l'Unione europea". La diffusione ed utilizzo dello standard è infatti uno degli obiettivi della direttiva 55 e in Italia sarà possibile utilizzare un tracciato più semplice di FatturaPA. Sarà SDI a tradurre le fatture inviate in formato UBL o CII in FatturaPA in modo da minimizzare i costi per le pubbliche amministrazioni.

Note conclusive

Secondo quanto indicato dalle nostre autorità nell'ambito di interviste che sono state realizzate per uno studio¹ commissionato dalla Commissione nel 2017, si pensa di mantenere un parallelo di qualche anno tra il formato italiano e quelli europei, quindi di dismettere entro 5 anni il formato FatturaPA in favore di UBL. L'obiettivo sembra fin troppo ottimistico ma l'obiettivo è tracciato, infatti l'obbligo di ordine elettronico in fase di introduzione mediante NSO (Nodo smistamento ordini) già prevede l'uso di UBL. Anche la convergenza del settore privato è inevitabile, sarebbe difficilmente sostenibile un progetto che si discosta in modo così netto dalla strada europea, in considerazione del Mercato Unico Digitale. L'introduzione dello standard europeo e la creazione del tavolo AgID stanno probabilmente creando situazioni di difficile gestione da parte delle autorità competenti. A pochi giorni dall'obbligo non è stato ancora pubblicato né il provvedimento del Direttore dell'Agenzia delle entrate (indispensabile per l'attuazione della direttiva), né il DPCM necessario per istituire il tavolo AgID, ma attendiamo fiduciosi.

¹ "Study on the practical application and implementation of the European e-Invoicing standard" disponibile al link <http://bit.ly/ESelInvStudy>

THE SCARECROW

Tendere verso le nuvole è davvero il suo unico destino?



di Luigi Foglia, avvocato

Segretario generale ad Interim di ANORC

Al fine di incrementare l'adozione di soluzioni informatiche in cloud da parte delle PA italiane, il Piano triennale per l'informatica nella pubblica amministrazione 2019-2021 ha disegnato un modello cloud ad hoc denominato "Cloud della PA".

La strategia cloud delineata da AGID prevede un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi Cloud alla Pubblica amministrazione, affinché queste ultime possano adottare servizi e infrastrutture di cloud computing omogenei, che rispettino elevati standard di sicurezza, efficienza ed affidabilità, in linea con le previsioni delle circolari AgID n.2 e n. 3 del 9 aprile 2018.

Viene così proposto alle PA italiane, sulla base del principio del cloud first, di valutare l'adozione di soluzioni cloud prima delle soluzioni tradizionali.

Il cloud, un insieme di tecnologie dai contorni purtroppo non ancora ben definiti (manca infatti nella normativa attuale una definizione chiara di cosa sia o non sia il cloud), è sicuramente un modello infrastrutturale in grado di agevolare in molte situazioni (ma non certo in tutte) il raggiungimento degli obiettivi di efficacia, efficienza ed economicità che dovrebbero animare l'agire amministrativo. Ben venga, quindi, un modello che sia in grado di aiutare le PA nella scelta delle soluzioni da adottare. Soprattutto laddove, ad oggi, non vi è alcun tipo di chiara regolamentazione della domanda/offerta di servizi informatici per le amministrazioni pubbliche.

Il cloud rientra sicuramente tra i vari modelli di offerta disponibili agli operatori. Il cloud buono, quello della PA previsto dal Piano Triennale e non quello "cattivo" fatto

a basso costo svendendo i nostri dati a grandi multinazionali o basato su risorse fisicamente disponibili in territori diversi da quello italiano: dopotutto stiamo parlando dei “nostri” dati, delle nostre informazioni nazionali.

Poi ci saranno sicuramente situazioni in cui il modello cloud della PA sarà il più efficiente, efficace ed economico e altri in cui, la sensibilità dei dati trattati, la natura delle attività svolte e la realtà nel quale tali sistemi vanno ad incidere, in cui sarà opportuno adottare soluzioni differenti. Solo la singola PA potrà effettuare, in tal senso, una scelta consapevole. Dopotutto, accanto a principi generali, sappiamo bene che le nostre PPAA agiscono sulla base di una propria autonomia regolamentare che le viene riconosciuta per legge proprio perché ogni PA insiste e agisce su realtà molto differenti tra loro.

Quello che occorrerebbe aumentare sono le competenze tecnologiche e informatiche delle nostre PA anche al fine di poter scegliere la giusta soluzione informatica da adottare. Dopotutto La Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle PA italiane conclude proprio ribadendo come *risulti urgente e non più procrastinabile un adeguamento delle competenze del personale (non solo) dirigenziale della PA, sia attraverso un massiccio investimento in formazione, sia attraverso una ineludibile immissione di nuovo personale*. L’istituzione dell’ufficio per la transizione digitale a costo zero non ha dato i frutti sperati. Bisogna investire. E lo sanno bene i soggetti pubblici e privati che fino ad oggi hanno investito per la qualificazione e l’accreditamento ex art. 29 del CAD dei loro servizi. Lo sa bene chi in AgID si è occupato in questi anni di accreditamento e vigilanza di tali servizi.

E per tali servizi, il modello Cloud per la PA è davvero un’opportunità?

In questi settori, ove la regolamentazione, europea e italiana, è già copiosa, serve davvero applicare un nuovo modello? Il rischio, in fondo, è quello di distorcere un mercato che dopo numerosi anni di disinteresse nei quali è **rimasto bloccato riuscendo a malapena a crescere**, si sta finalmente affermando come punto di riferimento nazionale e non, per garantire fiducia nelle transazioni elettroniche e nella conservazione nel tempo della nostra memoria informatica. Le attività di qualificazione e accreditamento portate avanti e affinate in questi anni, unitamente all’attività di vigilanza (che è sempre stata correttamente costruttiva e non distruttiva) han-

no permesso di raggiungere importanti obiettivi in termini di corretta erogazione di servizi efficaci, efficienti e anche economici (paragonati ai costi degli stessi servizi di altri paesi europei) alle PA italiane.

Un mercato fatto di piccoli e grandi player, in grado di lavorare sui grandi numeri così come su servizi iper-personalizzati: insomma, ad oggi ce n'è per tutti, per chi ha solo necessità di servizi base a basso costo e per chi, al contrario, la necessità di servizi ad alta integrazione e personalizzazione con quelli già presenti nella sua realtà.

In tale scenario, è davvero utile applicare il principio del *cloud first*? O si rischia, sull'onda di una *moda tecnologica*, di gettare al vento gli sforzi di molti operatori pubblici e privati fatti negli ultimi 15 anni?

Il cloud non è certamente il male, anzi. Anche per i servizi fiduciari e per la conservazione può rappresentare un giusto compromesso tra esigenze di funzionalità e di spesa per le PA. Proprio in tema di conservazione a norma dei documenti informatici, probabilmente si dovrebbe osare di più con le prossime Linee guida e aprire a soluzioni in cloud oggi, di fatto, non attuabili in base alle norme regolamentari e ai requisiti di qualità e sicurezza ad oggi richiesti per tali sistemi.

Le singole Amministrazioni pubbliche sceglieranno quando e se richiedere soluzioni in cloud e, in tal caso, i servizi scelti dovranno continuare a garantire i livelli di qualità e sicurezza già richiesti. Dovrebbero, infatti, essere gli stessi percorsi di qualificazione e accreditamento ad essere integrati per verificare la rispondenza delle soluzioni, adottate anche sfruttando il modello cloud, ai livelli di qualità e sicurezza richiesti. Diversamente, oltre a duplicare inutilmente percorsi e certificazioni, si finirebbe per non garantire un'applicazione omogenea di regole che, invece, dovrebbero garantire una corretta acquisizione di servizi informatici da parte delle PA italiane.



WHAT DO YOU WANT FROM ME

GDPR: un impegnativo, ma necessario, passaggio "dalla teoria alla pratica"



di Franco Cardin

Esperto privacy, Componente
del Direttivo ANORC

Coordinatore del Tavolo di Lavoro
ANORC "GDPR su processi
e sistemi di conservazione"

In occasione del DIG.Eat 2019 Franco Cardin affronta il lato oscuro della protezione dei dati personali, nel passaggio dalla "teoria" alla "pratica" applicativa di contesti pubblici e privati, richiamando l'attenzione sugli esiti del percorso condotto in ambito nazionale per l'adeguamento alla normativa europea e nazionale in materia. Il dott. Cardin presenta questa disamina all'indomani della conclusione del Tavolo di Lavoro ANORC 2018/19 sull'applicazione del GDPR, nel quale ha rivestito il ruolo di coordinatore.

Con l'edizione 2018 del DIG.Eat dal titolo "Digitalizzazione e Privacy: tutti compliant?" ci eravamo posti l'obiettivo di dimostrare che le tematiche dell'innovazione digitale e della protezione dei dati personali, non solo sono strettamente correlate, ma anche e soprattutto che non appartengono soltanto ai tecnici e agli esperti del settore ma riguardano inevitabilmente tutti coloro che sono coinvolti, con diversi ruoli e responsabilità, nei processi di miglioramento delle pubbliche amministrazioni o nell'elaborazione e implementazione delle strategie di business aziendali. Tale scelta era stata determinata - con particolare riferimento alla "privacy" - dall'avvicinarsi del fatidico 25 maggio 2018, data di piena applicabilità - dopo ben due anni dalla pubblicazione sulla Gazzetta Ufficiale della Comunità Europea - del Regolamento (UE) 2016/679, meglio

noto come GDPR. In quell'occasione i vari relatori, intervenuti per illustrare le principali novità introdotte dal nuovo regolamento europeo, avevano sottolineato che il 25 maggio 2018 non avrebbe rappresentato solo un obbligato punto di arrivo entro il quale i titolari e i responsabili del trattamento avrebbero dovuto essere in grado di dimostrare di essere compliant, ma anche e soprattutto sarebbe coinciso con **l'inizio di un nuovo approccio alla protezione dei dati personali** che - tenuto conto dell'introduzione del nuovo principio di responsabilizzazione (accountability) – avrebbe posto l'accento sull'effettività e la concretezza delle attività messe in atto per garantire la compliance o, per dirla con le parole del Gruppo di lavoro WP29, sulla necessità di passare **“dalla teoria alla pratica”** ¹.

Questo necessario passaggio dalla teoria alla pratica come è stato interpretato e realizzato dai titolari e dai responsabili del trattamento nei mesi successivi?

Alcuni dati, seppur parziali, emergono dall'indagine effettuata lo scorso settembre dall'Autorità di controllo del nostro Paese nell'ambito dello Sweep 2018 ², rispetto ai quali il Presidente Antonello Soro ha dichiarato **“I risultati dello Sweep 2018 confermano *che c'è ancora molto da fare* affinché i principi a tutela della privacy vengano declinati correttamente nelle pratiche quotidiane, nei processi organizzativi e lungo tutta la catena decisionale del settore pubblico e in quello privato”**.

Viene quindi spontaneo chiedersi: quali sono le ragioni che rendono difficile questo fondamentale passaggio **“dalla teoria alla pratica”**?

¹ Questa necessità è suggerita e motivata nel parere 3/2010 (WP 173) sul “principio di responsabilità” adottato il 13 luglio 2010 dal Gruppo di lavoro articolo 29 per la protezione dei dati.

² Per i risultati dell'indagine, che ha coinvolto tutte le Regioni e le Province autonome, nonché le rispettive società controllate, si veda il comunicato stampa del 5 marzo 2019 del Garante per la protezione dei dati personali (doc. web 9088164).

La prima e più importante ragione sta sicuramente nel fatto di **non aver acquisito la necessaria consapevolezza** che il pervasivo e inarrestabile processo di digitalizzazione che contraddistingue il mondo globalizzato - e che pervade ogni attività delle pubbliche amministrazioni e delle aziende private - ha avuto come effetto quello di aumentare il valore, sia sociale che economico, delle informazioni, con particolare riferimento a quelle riconducibili alle persone fisiche che, come è noto, rientrano nella definizione di dati personali.³

³ A conferma di questo aumentato valore, sia sociale che economico, dei dati personali è opportuno ricordare, da un lato il caso Cambridge Analytica e, dall'altro, la recente notizia ANSA secondo la quale il giornale L'Observer, citando alcuni documenti presi in visione, ha scritto che Facebook avrebbe tentato di esercitare pressioni su diversi politici in varie parti del mondo affinché facessero lobbying a favore dell'azienda contro le leggi sulla protezione dei dati.

Questa mancanza di consapevolezza è alla base di un comportamento, da parte ancora di molti titolari e responsabili del trattamento, caratterizzato dalla errata convinzione che la normativa in materia di "privacy" è un orpello burocratico che obbliga le aziende private e le pubbliche amministrazioni a sostenere inutili costi aggiuntivi sia per l'adeguamento organizzativo che tecnologico. Purtroppo, le notizie, oramai quotidiane, sul sempre più frequente e preoccupante fenomeno delle violazioni di dati personali (data breach) bastano da sole per dimostrare in che misura i costi erroneamente considerati "inutili" (utili a proteggere adeguatamente i dati personali), in realtà sono degli investimenti indispensabili, finalizzati a migliorare i servizi offerti dalle pubbliche amministrazioni e a favorire la crescita delle aziende private. Ebbene, quali dovrebbero essere le attività che ogni PA o azienda privata dovrebbe responsabilmente implementare per poter dimostrare di essere formalmente e sostanzialmente compliant con la normativa europea e nazionale in materia di protezione dei dati personali? Di seguito un breve ma indispensabile elenco:

- **rispettare** i principi di carattere generale contenuti nell'art. 5 del GDPR. Sembra un'ovvietà, ma invece troppo frequentemente questi principi - quali ad esempio quello di trasparenza, minimizzazione, limitazione della finalità e della conservazione - vengono sottovalutati. Il rispetto di questi principi comporta, prima di iniziare qualsiasi attività di trattamento di dati personali, la necessità di effettuare un adeguato processo di assessment finalizzato a mappare, le tipologie dei dati necessari, i loro flussi interni ed esterni all'organizzazione, nonché le modalità e i mezzi con i quali verranno trattati;
- **porre** al centro di qualsiasi attività che comporti il trattamento di dati personali il rispetto dei diritti e delle libertà fondamentali delle persone fisiche (dipendenti, clienti, pazienti, ecc.);
- **adottare** un approccio proattivo (*privacy by design e by default*) e non reattivo. Anche per le attività di trattamento dei dati personali è sicuramente meno costoso e utile prevenire piuttosto che correggere;
- **introdurre** all'interno delle organizzazioni la cultura del rischio e della sua gestione nell'ambito delle attività di trattamento dei dati personali.

Per concludere, un ultimo consiglio: il più grande errore che si possa fare - che poi in realtà rischia di diventare causa di significativi costi, non ultimo quello legato al venir meno della reputazione - è quello di pensare che sia possibile passare "dalla teoria alla pratica" senza una specifica, adeguata e continua formazione di tutti i soggetti che a vario titolo e con diversi ruoli e responsabilità effettuano, all'interno delle pubbliche amministrazioni e delle aziende private, operazioni di trattamento di dati personali.

ANY COLOUR YOU LIKE

Micromotivi e macrocomportamenti



di Giuseppe D'Acquisto

Funzionario direttivo - Garante
per la protezione dei dati personali

In occasione del DIG.Eat 2019 Giuseppe D'Acquisto presenta un intervento sul lato oscuro delle dinamiche dell'economia dei dati. Al centro della regolamentazione dei cosiddetti "Big Data" si colloca, oltre al trattamento dei dati delle persone, la capacità di fare previsioni comportamentali sulla base dei trattamenti di dati personali. Le nuove sfide non si preannunciano semplici.

La Dichiarazione del Consiglio d'Europa "*Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*" è un passaggio molto importante nella comprensione delle dinamiche dell'economia dei dati. L'oggetto nuovo della regolamentazione dei cosiddetti Big Data non è più tanto, o soltanto, il trattamento dei dati delle persone, ma la capacità di fare previsioni comportamentali sulla base dei trattamenti di dati personali. Magari anche comportamenti di altri. Osservare una persona per classificarla è tutto sommato un'attività di limitato interesse economico in sé. Ognuno di noi ha comportamenti molto ricorrenti da cui difficilmente si discosta: non prendiamo ogni giorno un percorso diverso per andare al lavoro, e molto probabilmente non acquisteremo il sushi se nell'ultimo anno non siamo mai stati a cena in un ristorante giapponese. Ciò che invece ha un enorme valore economico è la scoperta, un istante prima che ciò accada, dell'azione che siamo sul punto di intraprendere e che una buona previsione può mettere in luce, dando un grande vantaggio competitivo a chi arriva per primo alla scoperta. Ora, non c'è modo più efficace di prevedere un mio comportamento se non osservando gli altri: la prossima mossa che in me è inconsueta in altri può essere invece la norma, e questo rafforza l'efficacia della previsione. Naturalmente questo comporta ri-

schi enormi, che tutti possono facilmente comprendere. Il momento in cui decidiamo di “cambiare stato” (ad esempio, passare dallo stato di non acquirenti a quello di consumatore) è una fase di vulnerabilità per la persona, che può essere colta inducendola ad azioni non sempre a proprio vantaggio. Oggi si usa il termine di *nudging* (letteralmente, un piccolo incentivo) per indicare il piccolo tornaconto che può essere offerto alla persona per indurne questo cambio di stato. Sembra in questo nuovo lessico di riascoltare la lezione di Thomas Schelling, premio Nobel per l’economia nel 2005, che nei suoi studi degli anni ‘60 e ‘70 sulla teoria dei giochi per le decisioni strategiche aveva intuito il valore dei “*micromotives*” individuali che possono dare luogo a “*macrobehaviors*” collettivi. C’era già in questa grande intuizione tutto il meglio e tutto il peggio che ci si può aspettare oggi dai *Big Data*: la prospettiva di costruire una società più accogliente, grazie a incentivi a rimuovere barriere culturali o pregiudizi, ma anche il rischio di costruire una società di uguali, quasi automi, indotti tutti a compiere una stessa azione attraverso un *nudging* monocorde. Purtroppo non è possibile spezzare in due queste tecnologie di Big Data analytics: ciò che ci darà il meglio è anche ciò che ci potrà dare il peggio. Dunque serve un cambio di prospettiva comportamentale e culturale, dal quale dovranno discendere regole etiche e giuridiche nuove: questo è il messaggio del Consiglio d’Europa. Bisogna lavorare per tirare fuori il meglio da queste capacità predittive (il beneficio per le persone ci può essere, e questo è innegabile), evitando il peggio (ossia le *manipulative capabilities of algorithmic processes* di cui parla la Dichiarazione). Non sarà semplice. Il GDPR intuisce questi pericoli offrendo già oggi alle persone il diritto a non essere sottoposti a decisioni totalmente automatizzate e introducendo l’obbligo di pensare alla privacy sin dalla progettazione (la cosiddetta *privacy by design*), ma molto bisogna fare per costruire una reale responsabilizzazione sull’uso dei dati.

COMFORTABLY NUMB

Il lato oscuro... dell'analisi del rischio



di Enrico Pelino

Privacy Expert e componente del Consiglio
Direttivo di ANORC Professioni

In occasione del DIG.Eat 2019 Enrico Pelino propone una digressione sul lato oscuro dell'analisi del rischio, che può giungere al paradosso di divenire essa stessa un rischio. Presenta il caso di una sentenza di condanna statunitense basata sugli esiti di una valutazione automatizzata condotta da un software, la cui logica è coperta da segreto industriale. Ebbene, la nuova frontiera del diritto è quella di pretendere una logica accessibile delle macchine, muovendo uno sforzo concreto per renderla intelligibile ai destinatari umani.

L'analisi del rischio è attività pervasiva nel Regolamento e affiora in molteplici istituti. Del resto, la nozione di rischio, ossia l'oggetto di tale analisi, costituisce la stella polare per orientare l'*accountability*. Nessuna norma impone di condurre l'analisi del rischio attraverso modelli di calcolo automatizzati o parzialmente automatizzati, come ad esempio quelli di Enisa, e non piuttosto secondo una valutazione più discorsiva, umana, non computazionale. Ricorrere ai modelli di calcolo automatizzati vuol dire usare algoritmi decisionali, ossia selezionare determinati elementi d'ingresso considerati rilevanti, attribuire loro un peso numerico, seguire uno schema fisso di passaggi, calcolare il risultato secondo una formula e collegarvi determinate conseguenze operative.

Descritti così, questi modelli di *risk-assessment* sono in tutto e per tutto processi decisionali automatizzati, anche quando non abbiano ad oggetto una persona fisica, ma la predisposizione di misure di sicurezza. In quanto tali, presentano vantaggi e svantaggi tipici. Tra i vantaggi ci sono quelli di presentare processi misurabili, impermeabili alla soggettività dell'operatore, facilmente dimostrabili all'autorità di

controllo. Gli svantaggi sono, a ben guardare, esattamente gli stessi, ma in un'ottica rovesciata: fornire rassicuranti automatismi che dispensano da ragionamenti più profondi e sartoriali; ultra-semplificare realtà complesse; non correggere eventuali vizi d'impostazione dell'algoritmo attraverso il filtro della soggettività dell'operatore. Soprattutto, nessuno ci informa di un piccolo paradosso, ossia che l'analisi del rischio condotta attraverso algoritmi può costituire un rischio essa stessa, specialmente quando l'oggetto cui si applica è la valutazione diretta di persone fisiche e quando il processo risulta interamente automatizzato.

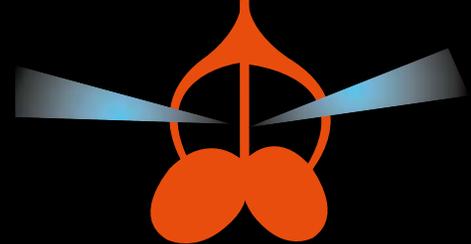
Eppure, basterebbe chiedere a Eric L. Loomis, o meglio ai suoi avvocati. La vicenda che lo riguarda è efficacemente riassunta dal titolo di un articolo della giurista Rebecca Wexler apparso un paio di anni fa (13 luglio 2017) sul New York Times: *"When a Computer Program Keeps You in Jail"*, quando un software ti tiene in galera. Già perché se il sig. Loomis è stato condannato a una pena detentiva di sei anni, l'elemento determinante è stato proprio un'analisi del rischio. Ben fatta, predittiva, attuariale. Il problema di Loomis (nel sistema penale statunitense) è quello di avere ottenuto un punteggio alto nella scala "Compas", quello dei suoi avvocati di non sapere perché. La logica alla base di Compas è infatti un segreto industriale della società che l'ha creato e lo distribuisce. Detto altrimenti: è una black box informatica che produce valutazioni, senza che sia possibile ricostruirne il sottostante percorso motivazionale, vale a dire la logica applicata nei calcoli e nella ponderazione. La logica è la chiave, non a caso il diritto a ottenere "informazioni significative sulla logica utilizzata" costituisce, nella normativa europea, il cuore degli artt. 13.2.f, 14.2.g, 15.1.h GDPR. La logica è tutto: come si può infatti "ottenere un intervento umano", "esprimere la propria opinione", "contestare la decisione", ossia esercitare le fondamentali pretese riconosciute dall'art. 22.3 GDPR nel caso di decisioni interamente automatizzate, se si opera alla cieca? La vicenda Glenn Rodríguez è esemplare in questo senso. Ce la racconta sempre la nostra Rebecca Wexler. Rodríguez è un detenuto che si è visto negare la liberazione condizionale a causa di un elevato punteggio Compas, nonostante una condotta irreprensibile in carcere, mentre il beneficio era stato concesso, in base allo stesso strumento di *risk-assessment*, a soggetti coinvolti in episodi violenti durante il periodo di detenzione. Qualcosa di incomprensibile nel suo punteggio Compas penalizzava dunque il sig. Rodríguez,

ma che cosa? La logica dello strumento gli era preclusa, costringendolo a lavorare per ipotesi, su raffronti esterni. Confrontandosi con altri detenuti attraverso una rete di solidarietà e collegando le domande di input di ciascuno con i rispettivi risultati finali, Rodríguez alla fine ha individuato un errore in uno degli input immessi nella sua valutazione. Tuttavia, non è riuscito a dimostrare il peso dirimente di questo errore sull'esito finale in quanto non ha avuto accesso alla logica sottostante, ha potuto solo immaginarla. Come scrive la Wexler, *“senza conoscere il peso assegnato a ciascun input, non era in grado di spiegare gli effetti dell'errore e di persuadere qualcuno a correggerlo”*. Il diritto di conoscere la logica è dunque determinante. Ma neppure questo basta, perché la logica, se costruita su modelli matematici, può essere estremamente complessa. Occorre che la logica sia anche *intelligibile*. Occorre cioè uno sforzo concreto per trasferirla in termini umani: la trasparenza non è nulla se non è calibrata sul destinatario. Pretendere una logica accessibile e *intelligibile*: questa è esattamente una delle nuove frontiere del diritto, su cui lavorare come giuristi nel brevissimo periodo, anzi già nel presente. Paul de Laat, in un articolo relativamente recente (*Big data and algorithmic decision-making: can transparency restore accountability?*, settembre 2017) esamina i pericoli di rivelare la logica dell'algoritmo, tra i quali la possibilità di ingannarlo conoscendone il funzionamento, ma appunto – potrà ben obiettersi – ingannare l'algoritmo non è forse un diritto soggettivo che dovrebbe essere proclamato tra quelli fondamentali e non certo temuto? Un algoritmo che può essere ingannato è infatti un algoritmo che inganna, non è un buon algoritmo, come una legge che può essere aggirata non è una buona legge: aggirare, paradossalmente, permette di migliorare e affinare. Come scrive Cathy O'Neill in *Weapons of Math Destruction*, p. 18: *“Conditions change, and so must the model”*. Doverose note di chiusura: ovviamente i modelli Enisa sono trasparenti e verificabili e l'autore li applica con entusiasmo. L'art. 22.3 GDPR presenta, a parere di chi scrive, una notevole falla che merita riflessione: non si applica ai processi decisionali interamente automatizzati autorizzati *ex lege*.

BREATHE

La conservazione by design

BREATHE



di Giuseppe Vitrani

Avvocato, esperto in privacy e Componente di D&L NET

In occasione del DIG.Eat 2019 Giuseppe Vitrani affronta il lato oscuro della protezione dei dati personali, con l'obiettivo di analizzare le interazioni che possono stabilirsi tra la normativa sul trattamento dei dati personali e il mondo degli archivi digitali, al fine di verificare se il rispetto dei principi di accountability, che gravano sul titolare del trattamento, possa essere assicurato anche da soluzioni archivistiche

Don't be afraid to care

Non aver paura di preoccuparti, ci insegnano i Pink Floyd in "Breathe"; il verso è quanto mai appropriato ai tempi dell'*accountability* prevista dal GDPR e ispira una riflessione circa gli strumenti informatici che possono alleviare le giuste preoccupazioni del buon titolare (o responsabile) del trattamento.

Liberi dunque dalla paura di preoccuparsi: si può guardare con fiducia al mondo degli archivi digitali, forse ancora poco conosciuto dal mondo privato, ma foriero di grandi potenzialità anche in ottica di *compliance* al GDPR.

Attraverso gli strumenti messi a disposizione dalla tecnologia è possibile infatti fornire delle buone risposte in termini di *data retention* e di rispetto del diritto alla portabilità dei dati personali di cui all'art. 21 del regolamento europeo, oltreché di successivo scarto dei dati personali per i quali siano decorsi i termini di conservazione.

Gli archivi digitali e il diritto alla portabilità

Una prima riflessione la si può compiere partendo dal diritto alla portabilità dei dati personali codificato nell'art. 21 del Regolamento UE n. 679/2016, il cui primo comma recita:

“l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti”.

Quando ci si interroga su quale sia la migliore risorsa in grado di assicurare questo diritto non si può non pensare alla struttura degli archivi digitali, così come delineata dal codice dell'amministrazione digitale e (attualmente) dal dpcm 3 dicembre '13.

Si può così riflettere sul fatto che il pacchetto di archiviazione è improntato alla piena interoperabilità, grazie alla presenza al suo interno del cosiddetto “indice del pacchetto di archiviazione”, ovvero di una struttura che fa riferimento allo standard SInCRO, che è lo standard nazionale riguardante l'insieme dei dati a supporto del processo di conservazione ed è formato con l'utilizzo di file XML (ovvero un formato strutturato, di uso comune e leggibile da dispositivo automatico, come richiede il GDPR).

A fronte dell'esercizio del diritto in questione, ben si può pensare di rispondere attraverso l'esibizione di dati (o documenti) correttamente archiviati, proprio perché al soggetto interessato al trattamento tali dati verranno consegnati o trasmessi con modalità tali che potranno essere conferiti ad un altro archivio senza alcun problema di interoperabilità.

Gli archivi digitali e la data retention

In secondo luogo non si può non considerare che una delle obbligazioni del titolare del trattamento è quella di determinare (e rispettare) il periodo di conservazione dei dati personali; una sfida difficile da rispettare soprattutto quando i dati sono disseminati su varie piattaforme o magari anche su differenti servizi *cloud*. Anche in tale ottica l'accentramento dello *storage* dei dati all'interno degli ar-

chivi digitali appare una soluzione da studiare con attenzione perché può dare ottime risposte in termini di compliance al Regolamento europeo.

La realtà ci dice che molto spesso i soggetti che scelgono di custodire i propri documenti all'interno di archivi digitali lo fanno ricorrendo a servizi in outsourcing e dunque affidandosi a soggetti privati, il più delle volte in possesso di accreditamento da parte di AgID. Si tratta innanzitutto di una scelta premiale in termini di *accountability*, stante che in tal modo i dati personali (oltre che i documenti) vengono affidati ad un soggetto che, innanzitutto, è sottoposto ad un rigido controllo da parte di un'autorità governativa.

Inoltre, va considerato che l'affidamento dei dati al conservatore avviene mediante la stipula di un contratto, uno dei cui elementi essenziali sono la determinazione del periodo di tenuta dei documenti da parte di quest'ultimo e la regolamentazione della sorte dei documenti una volta spirato il suddetto termine: restituzione al soggetto produttore o scarto definitivo.

È evidente come anche in tal caso vi siano delle naturali ricadute positive in termini di gestione della privacy e per renderlo evidente è sufficiente ricorrere ad un esempio.

L'art. 31, comma terzo, del decreto legislativo n. 231 del 2007, che detta disposizioni in materia di antiriciclaggio, prevede ad esempio espressamente che "i documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale".

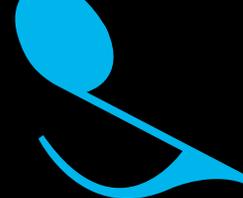
Nel caso specifico, i soggetti obbligati alle verifiche antiriciclaggio raccolgono molti dati personali dei propri clienti e dunque devono preoccuparsi della loro custodia per un tempo predefinito per legge.

Ebbene, nel momento in cui tali dati, che nella quasi totalità dei casi sono memorizzati su documenti informatici, vengano correttamente archiviati con le modalità sopra descritte, si genererà un effetto positivo anche in termini di rispetto della *data retention*. Il contratto con il conservatore conterrà l'espressa previsione del termine decennale di conservazione e pertanto, allo spirare dello stesso, vi sarà un soggetto terzo che in maniera automatizzata ricorderà al soggetto produttore la scadenza. A questo punto egli potrà decidere la sorte dei

documenti e dei dati in essi racchiusi e, ove non vi sia più alcun interesse residuo alla detenzione degli stessi, ne autorizzerà lo scarto; scarto che verrà eseguito direttamente dal conservatore, anche in tal caso secondo precise procedure rispettose anche della normativa in tema di trattamento dei dati personali. Questi semplici esempi rendono evidente come il mondo degli archivi, soprattutto di quelli digitali, possa offrire validissime risposte in termini di *privacy by design*. Ma non bisogna neppure dimenticare le positive ricadute in termini di *privacy by default*: se i dati vengono raccolti con la prospettiva di dover poi confluire in un archivio tenuto a norma del Codice dell'Amministrazione Digitale delle regole tecniche attuative (in futuro, Linee Guida), già dalla fase di impostazione non si potrà prescindere dall'utilizzo di formati documentali aperti, interoperabili e non proprietari (essendo i soli per i quali si può prospettare un'efficace strategia di conservazione). In virtù di tali scelte sarà dunque possibile rispondere con maggiore efficacia alle richieste di esercizio del diritto alla portabilità dei dati da parte del soggetto interessato al trattamento.

In conclusione

In conclusione si può dunque affermare, riprendendo il tema di inizio articolo, che il titolare (o responsabile) del trattamento non deve aver paura di preoccuparsi, ma deve invece sfruttare questa giusta paura per sviluppare i migliori presidi (nel caso di specie, in tema di normativa privacy) a tutela della propria organizzazione.



di Michele Iaselli

Avvocato, esperto privacy e Presidente di ANDIP

In occasione del DIG.Eat 2019 Michele Iaselli, presenta un intervento sul lato oscuro dell'introduzione di nuove tecnologie. In risposta alla continua evoluzione è necessario predeterminare un quadro etico e giuridico corretto utile per consentire l'adozione di regole appropriate e gestire il corretto recepimento delle novità in ambito nazionale.

Il divario temporale tra l'emergere di una tecnologia e la sua successiva regolamentazione non può essere valutato, in determinati casi, in termini completamente negativi poiché consente di avere più tempo per comprendere le possibili conseguenze e condurre, così, a decisioni politiche più corrette e consapevoli. E' necessario difatti, anche prevedendo rischi futuri di attività che sono in continua evoluzione, predeterminare un quadro etico e giuridico corretto utile per consentire l'adozione di regole appropriate ed orientare i successivi processi di ricerca e di produzione con valori etici e legali riconosciuti a cui la progettazione di prodotti innovativi si debba conformare.

La novità di maggior rilievo dal punto di vista giuridico-tecnologico della recente conversione in L. n. 12/2019, con modificazioni, del DL 14 dicembre 2018, n. 135, è sicuramente rappresentata dall'art. 8-ter, che definisce le **tecnologie basate sui registri distribuiti e gli smart contract**.

Questi ultimi, in particolare, sono in grado di soddisfare il requisito della forma scritta previa identificazione informatica delle parti interessate. Inoltre, è bene sottolineare che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti, produce gli effetti giuridici della

validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (Regolamento eIDAS).

Come poi spesso accade quando si definiscono aspetti di natura fortemente tecnologica si rinvia a standard tecnici (che dovranno essere definiti dall'Agenzia per l'Italia Digitale entro 90 giorni) dall'entrata in vigore della legge per sapere quali debbano essere le caratteristiche utili a produrre gli effetti giuridici menzionati in precedenza.

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

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

Gli *Smart Contract* potrebbero essere una risorsa molto importante nella gestione dei documenti presenti nel procedimento amministrativo della PA per le loro caratteristiche di sicurezza e trasparenza, per quanto, allo stato attuale dell'arte, gli stessi *Smart Contract* risultano avere dei problemi legati alla struttura pubblica e decentralizzata della *blockchain*, nel tempo stesso punto di forza e di debolezza della stessa.

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

rendendone l'utilizzo, ad oggi, complesso e costoso.

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

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

La predisposizione di un sistema contraddistinto da tale tecnologia implica, inevitabilmente, nell'ottica dei principi generali del GDPR sopra evidenziati, uno studio approfondito sui rischi, non di poco conto, connessi in materia di protezione dei dati personali per cui sarebbe necessario quanto meno condurre un'accorta valutazione di impatto sulla protezione dei dati personali alla luce dell'art. 35 del GDPR che tenga conto delle specifiche peculiarità dello strumento tecnologico. In altri termini è giusto come sottolineato dalla Commissione europea studiare ed approfondire tali tecnologie ma non giungere a conclusioni troppo affrettate visto che il nostro Paese ha già vissuto precedenti esperienze (vedi la firma digitale o la posta elettronica certificata) per le quali ha anticipato l'introduzione e la regolamentazione di tecnologie rimanendo però drammaticamente isolato per la mancata condivisione nell'ambito dell'Unione europea.



Firmiamo da sempre, non eravamo ancora maggiorenni
e già firmavamo digitalmente in Cloud
per circa 200 milioni di volte l'anno.

ORA CHE NE ABBIAMO PIÙ DI 25 VI FAREMO DIVERTIRE...



SIGN DIFFERENT **HAPPYSIGN**

L'applicazione di verifica è ora supportata da una interfaccia web piena di funzionalità innovative



HONOS

- Controllo dei Documenti e delle Firme Digitali
- Apposizione Firma Digitale
- Apposizione FEA Glifometrica



HAPPYSIGN

- Gestione SignAutomation dei cicli Approvativi
- Firma Digitale anche Multipla
- Applicazione Contrassegno Elettronico su documenti già Firmati
- Gestione Firma Documenti con Apperance dinamica ed Attachment
- Collaborazione con Applicativi esterni
- Visualizzazione documenti a supporto
- Gestione delle pratiche
- Archivio documenti
- Gestione del Registro di Validità dei singoli documenti

LAND S.r.l.

Via di Affogalasino, 40

00148 ROMA

info@land.it - www.land.it



Egov e Sanità

Privacy e Sicurezza

Archivi Digitali

Ebusiness e Contratti

Academy e Formazione

studiolegalelisi.it

Lecce - Milano

segreteria@studiolegalelisi.it



Corsi

In House

In presenza

e-learning

streaming

studiolegalelisi.it/academy

Partner dei nostri progetti
di formazione:



Da oltre 10 anni rappresentiamo i bisogni di società, enti pubblici, professionisti ed esperti del settore della digitalizzazione e della privacy.



Link: <https://www.anorc.eu/>



Conservazione digitale

eWitness
Certezze Digitali

Diamo valore legale ai tuoi
documenti digitali.

ewitness.eu





Entra nella nostra rete **AGENZIA IMPRESA**

Lavora con noi diventando un professionista del DIGITALE! Affiliandoti alla nostra rete avrai tutti gli strumenti necessari per poter operare totalmente in autonomia.

Ti forniremo: **Una tua piattaforma in cloud, Supporto tecnico commerciale, Formazione, Strumenti di marketing.**

Richiedici informazioni:

www.agenziaimpresa.com

Per digitalizzare i tuoi processi aziendali. Scegli **AGENZIA IMPRESA**

Affidandoti ad un nostro affiliato potrai ricevere consulenza a 360° unitamente ai servizi necessari per gestire in modo completo la digitalizzazione della tua azienda o del tuo studio professionale. Scegli un nostro affiliato:

www.agenziaimpresa.com

I NOSTRI SERVIZI DIGITALI

Ecc **D**oc

Conservazione digitale dei documenti informatici

Ecc **F**att

Fatturazione Elettronica

Ecc **P**ec

Gestione a norma delle PEC

Ecc **F**irm

Firma Digitale Remota

Ecc **P**a

Adempimenti Telematici rivolti alla PA

Ecc **P**rivacy

Adempimenti in materia di Privacy



agenziaimpresa
digitale.

WELCOME TO THE MACHINE

WELCOME
TO THE
MACHINE



di Davide Maniscalco

Avvocato - componente del D&L NET e referente territoriale di ANORC Professioni



In occasione del DIG.Eat 2019 Davide Maniscalco, presenta un intervento sul lato oscuro del dominio cibernetico, in prospettiva dell'introduzione di standard europei per la certificazione di prodotti e processi. La *security by design* costituirà, insieme alla *privacy by design*, un requisito essenziale per i Titolari ed i Responsabili del trattamento, soprattutto, in materia di appalti pubblici.

La recente intesa politica tra le istituzioni dell'Unione Europea circa il testo del nuovo Regolamento, noto come *Cybersecurity Act*, favorirà la realizzazione di un Mercato unico digitale, con l'introduzione di standard europei per la certificazione di prodotti e processi afferenti alla protezione del dominio cibernetico, secondo il paradigma, invero mutuato dal Regolamento (UE) 2016/679, della *security by design*. Non vi è dubbio che in punto di progettazione dell'architettura della sicurezza, entrambe le normative regolamentari presentino un denominatore comune, che trae origine dalla **esigenza di proteggere i dati "sensibili" che possono costituire anche patrimonio informativo delle aziende produttrici**, nonché informazioni classificate degli operatori dei servizi essenziali o di fornitori di servizi digitali, intesi questi ultimi come infrastrutture critiche per la loro importanza strategica e, talvolta, per la sicurezza nazionale.

In questo scenario, anche **il tema della privacy by design disciplinato dal GDPR, dovrà essere sempre più integrato nella nuova accezione di security by design**, ed

in quanto principio fondamentale di tutela, costituirà un requisito essenziale per i Titolari ed i Responsabili del trattamento, soprattutto, in materia di appalti pubblici. D'altronde, il paragrafo 3 dell'art. 25 del GDPR, andava già in questa direzione, prevedendo un meccanismo di certificazione approvato ai sensi dell'articolo 42, come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2.

E' bene a questo proposito ricordare che l'art. 25 del GDPR si rivolge al Titolare , sancendone l'obbligo, sia **al momento di determinare i mezzi**, che all'atto del trattamento stesso, di mettere in atto misure tecniche e organizzative adeguate (quali la pseudonimizzazione e la minimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie utili soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati. Il Titolare dovrà tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

E' dunque importante, nell'accezione più ampia della *security by design*, operare una integrazione tra i due concetti, estendendo altresì analogicamente l'obbligo previsto dall'art. 25 del GDPR, nella sua fase "infrastrutturale" al Responsabile del trattamento. Ed infatti, dal tenore letterale dell'art. 28 del GDPR si evince per il quest'ultimo l'enunciazione di un principio certamente coerente con la finalità della *privacy by design*, vale a dire il criterio di "individuazione", determinato sulla base della circostanza che si presentino o meno garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in ordine alla tutela dei diritti degli interessati. Ne consegue che l'obbligo di *privacy by design*, nella cornice del più ampio e generale principio di *accountability* del Titolare del trattamento, non può certamente ritenersi avulso anche dalla sfera giuridica del Responsabile del trattamento. **In ragione della rinnovata condivisione di compiti e della nuova configurazione del mercato unico digitale voluta dall'UE, si gioca la partita tra committenti Titolari e fornitori/Responsabili di prodotti e servizi digitali, nella cornice di standards europei di certificazione di software e processi.**

L'integrazione dei concetti di privacy by design e security by design rappresenta quindi l'evoluzione "infrastrutturale" by design dell'information security, consentendo la piena efficacia del principio di accountability nell'ambito di un sistema di garanzie, che aumenterà i livelli di fiducia degli utenti del mercato unico digitale.

Dunque, il Titolare del trattamento nell'adottare una privacy policy compliant rispetto al principio di privacy by design, potrà essere ritenuto efficacemente accountable, allorquando andrà a fruire di prodotti o servizi la cui progettazione sia by design certificabile e conforme a standards europei dettati dal Cybersecurity Act.

Nel nuovo scenario che verrà a configurarsi, pertanto, le garanzie sufficienti richieste dall'art. 28 del GDPR per l'individuazione del Responsabile del trattamento, discenderanno auspicabilmente da un sistema di certificazione europeo che garantirà la sicurezza by design di prodotti, servizi ed applicazioni, di guisa da assicurare al Titolare del trattamento, un livello certificato o certificabile di affidamento nella scelta e, dunque, la piena efficacia della sua accountability.

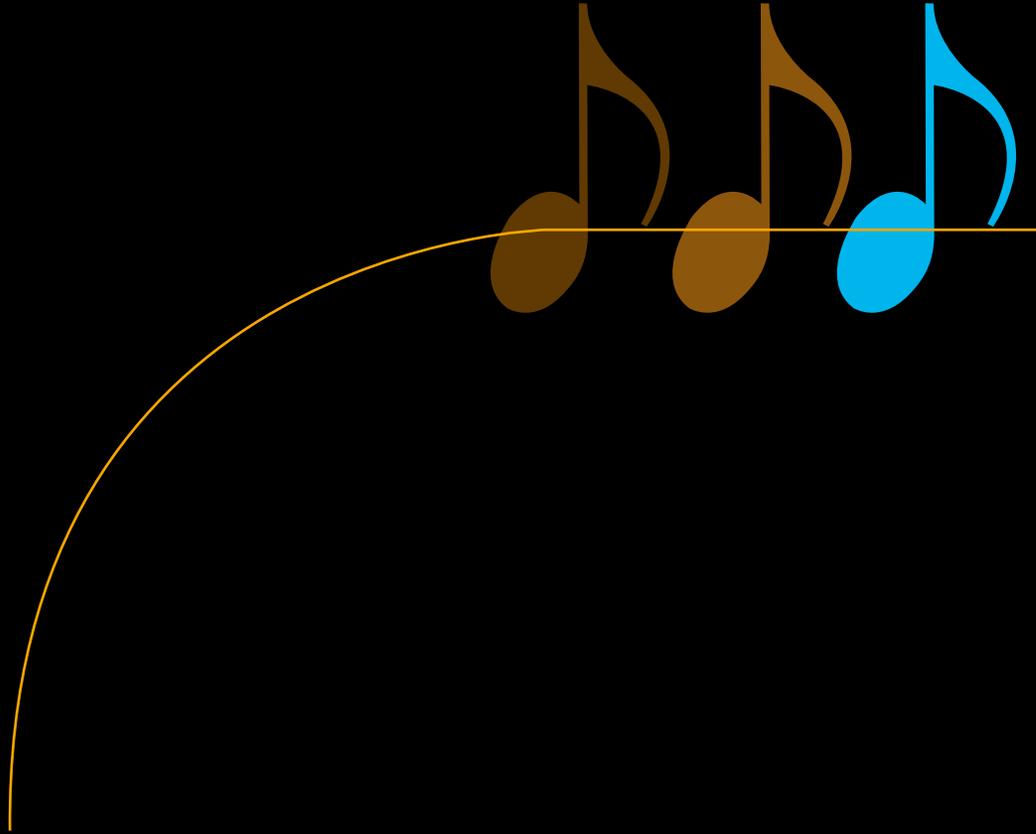
Non vi è dubbio che la sicurezza by design di prodotti e processi nel mercato unico digitale, cristallizzerà la responsabilità del produttore/Responsabile e, ciò, in stretta connessione, renderà certamente più agevole al Titolare del trattamento la dimostrazione dell'adeguatezza delle misure di sicurezza messe in campo, esattamente come previsto dall'art. 24 del GDPR.

Ecco che nella previsione dello standard di certificazione nel mercato unico digitale, trova applicazione anche il lungimirante contenuto del Considerando 78 nella parte in cui incoraggia i produttori a tener conto della protezione dei dati (ed oggi anche della security by design) al momento dello sviluppo e/o della progettazione di tali prodotti, servizi o applicazioni.

La piena attuazione del mercato unico digitale accrescerà, dunque, la fiducia dei cittadini e delle imprese nella società digitale e, permetterà di sviluppare ulteriore sicurezza nell'ambiente digitale, come logico presupposto per beneficiare in pieno dell'economia digitale europea.

Tale fiducia, in ambito privacy, si tradurrà in una certezza misurabile della discipli-

na contrattuale dei rapporti tra Titolare e Responsabile in ordine ai prodotti, servizi ed applicazioni forniti da quest'ultimo, la cui progettazione risulterà garantita da standard europei di certificazione da un lato opponibili dal Responsabile del trattamento ai sensi dell'articolo 28 del GDPR e, dall'altro, dimostrabili dal Titolare del trattamento, ai sensi dell'art. 25 del Regolamento.





di Sarah Ungaro

Avvocato – Vicepresidente di ANORC Professioni

In occasione del DIG.Eat 2019 Sarah Ungaro affronta il lato oscuro del Cloud First, con una riflessione sulle linee di azione contenute nel Piano triennale per l'informatica della Pubblica Amministrazione e le sfide che attendono il futuro delle nostre PA

*[All you save/and all that you give/and all that you deal/and all that you buy/beg, borrow or steal...]*¹

Dalla lettura dell'ultimo Piano triennale per l'informatica della Pubblica Amministrazione (2019-2021) sembra emergere chiaramente che il **mantra per il futuro digitale della PA italiana risponda al principio del Cloud First**. Ovviamente, tale strategia implicherà non solo una trasformazione radicale delle infrastrutture utilizzate, ma avrà anche un **impatto di rilievo sull'implementazione di servizi e sulla gestione dei procedimenti amministrativi, comportando il sovvertimento delle dinamiche che finora hanno animato la gestione dei dati pubblici**.

Tutto questo, però, dovrà avvenire senza mai dimenticare due presupposti fondamentali: **la sicurezza informatica e la protezione dei dati personali**.

Ma quali sono i punti cardine dello scenario delineato nel Piano triennale per attuare – concretamente - la strategia del Cloud First? Sicuramente, è possibile sintetizzare le linee d'azione descritte nel documento in questi obiettivi:

- **censimento** e conseguente **razionalizzazione** delle infrastrutture IT esistenti, finalizzati alla migrazione in Cloud dei sistemi informativi delle PA e alla progettazione e realizzazione di data center nell'ambito di Poli strategici nazionali

- **attuazione** del Programma nazionale di abilitazione al Cloud della PA (*Cloud Enablement Program*)
- **qualificazione** di infrastrutture e servizi da parte di AgID, che confluiranno sulla piattaforma Cloud Marketplace
- **aggiornamento** del modello di connettività

Razionalizzazione delle infrastrutture IT esistenti migrazione in Cloud, Poli Strategici Nazionali

Per quanto attiene alla razionalizzazione delle infrastrutture IT esistenti, è necessario considerare che il punto di partenza è il censimento del patrimonio ICT della PA, avviato con la Circolare AgID n. 5 del 30 novembre 2017. All'esito del censimento, le infrastrutture vagliate sono classificate in 3 categorie:

- candidabili a Poli strategici nazionali, ossia idonei a costituire quell'insieme di infrastrutture IT (centralizzate o distribuite) ad alta disponibilità, di proprietà pubblica, eletti quali Poli Strategici Nazionali dalla Presidenza del Consiglio dei Ministri e qualificati da AGID per erogare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali on-demand, servizi di disaster recovery e business continuity, servizi di gestione della sicurezza IT ed assistenza ai fruitori dei servizi erogati;
- Data center di qualità, ma non idonei come Poli strategici nazionali, oppure con carenze strutturali o organizzative minori (**gruppo A**);
- Data center che non garantiscono i requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo o non garantiscono la continuità dei servizi (**gruppo B**).

L'obiettivo è quello di **pianificare il consolidamento dei Data center del gruppo A** (i piani di migrazione in Cloud di ogni PA dovranno essere trasmessi ad AgID en-

tro novembre 2020) e la dismissione dei Data center del gruppo B (entro giugno 2020 le PA interessate dovranno dare comunicazione ad AgID della dismissione di tali Data center).

Programma nazionale di abilitazione al Cloud della PA

Con l'obiettivo di agevolare l'adozione del Cloud della PA, AgID e il Team per la trasformazione digitale hanno avviato il *Cloud Enablement Program*, finalizzato all'adozione prioritaria del paradigma cloud per la definizione di qualsiasi nuovo progetto o lo sviluppo di un servizio da parte delle PA.

In concreto, entro maggio 2019 è attesa - da parte di AgID e del Team - la pubblicazione in consultazione delle **Linee guida per lo sviluppo di servizi cloud native per il Cloud della PA**, mentre, entro novembre 2019, la pubblicazione in consultazione delle Linee guida per il modello di abilitazione e migrazione al Cloud della PA e la definizione dei centri di competenze.

I primi contratti a supporto del Programma di abilitazione al Cloud della PA sono attesi entro dicembre 2020, stipulati tramite apposite gare strategiche di Consip (Public Cloud e Digital Trasformation).

Qualificazione di infrastrutture e servizi cloud da parte di AgID

Il Modello Cloud della PA (introdotto dal Piano triennale 2017-2019) ha previsto un insieme di infrastrutture IT e di servizi cloud qualificati da AgID a disposizione delle PA e consultabili mediante il Cloud Marketplace. Il conseguimento delle qualificazioni di Infrastrutture e servizi, nello specifico, sono oggetto delle Circolari n. 2 e n. 3 del 2018 di AgID.

In particolare, i servizi qualificati saranno disponibili in modalità IaaS (Infrastructure as a Service), PaaS (Platform as a Service) e SaaS (Software as a Service) e saranno erogati tramite infrastrutture qualificate: i Cloud Service Provider qualificati da AgID, i Poli Strategici Nazionali e l'infrastruttura di Community Cloud realizzata dagli aggiudicatari del relativo contratto quadro Consip.

Connettività

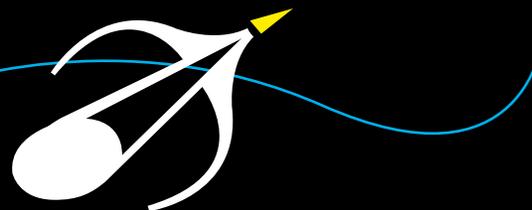
In riferimento all'adeguamento della connettività, il Piano triennale individua quattro direttrici principali:

1. **potenziare** la capacità di connessione delle amministrazioni, anche avvalendosi di infrastrutture di rete virtualizzate;
2. **consentire** alle sedi delle pubbliche amministrazioni di accedere a internet e ai servizi cloud;
3. **permettere** l'interconnessione dei Poli Strategici Nazionali;
4. **favorire** la fruizione dei servizi pubblici da parte di cittadini e imprese.

A fronte di tali ambiziosi obiettivi, **risulta imprescindibile un'attenta valutazione circa le misure tecniche e organizzative necessarie a garantire la sicurezza delle infrastrutture e dei servizi erogati in cloud**, anche nella prospettiva di una completa conformità dei trattamenti di dati personali effettuati -in cloud - dalle nostre PA alle norme del Regolamento 2016/679/UE in materia di protezione dei dati personali.

¹ Dal brano Eclipse, dall'album The Dark Side of the Moon, Pink Floyd, 1973.

A GREAT DAY FOR FREEDOM



La fatturazione elettronica come opportunità per l'innovazione dei processi aziendali.



di Rosario Farina

Responsabile Fatturazione Elettronica e Conservazione Digitale Gruppo Enel e Responsabile Contabilità Generale Country Italy Enel.

In occasione del DIG.Eat 2019 Rosario Farina presenta un intervento sul lato oscuro della fatturazione elettronica. Di fatturazione si può soffrire, sopravvivere o crescere. Le informazioni contenute nel tracciato possono diventare il volano verso una partnership innovativa con clienti e fornitori, attraverso scambi digitali di dati con modalità facilmente fruibili dalle imprese.

Fatturazione elettronica: il valore sta nell'informazione non nel contenitore

Dopo diversi mesi dall'avvio (obbligatorio dal 1° gennaio 2019), la fatturazione elettronica è ancora percepita come un mero adempimento e non come opportunità, rapida ed efficiente, di relazione tra imprese.

È uno tsunami oppure un mare navigabile per approdare verso nuovi e affascinanti porti? È una questione di approccio e di visione evolutiva dei processi. Nel primo caso, la fatturazione elettronica verrà vista come un costo ed un adempimento osteggiato e criticato, nel secondo, diventerà un viatico per la crescita aziendale grazie all'innovazione dei processi, facilitata dalla digitalizzazione.

In questi mesi ho visto sguardi di commercialisti e imprese persi nel vuoto, slogan sui social (anche divertenti: "con la sigaretta elettronica smetti di fumare con la fatturazione elettronica smetti di fatturare"), ma ho anche assistito a casi di evoluzio-

ne ed innovazione dei processi, nel momento gli “addetti ai lavori” hanno smesso di considerare la **fattura elettronica come mero contenitore elettronico, per ripensarla quale “cornucopia”** delle preziose informazioni presenti nel tracciato.

Scendere nel dettaglio delle informazioni che possono comporre il file fattura significa non limitarsi ad indicare le informazioni obbligatorie, in quanto richieste dalle normative fiscali, ma al contrario comprendere quali dati è utile individuare e movimentare nel tracciato così da soddisfare le esigenze di interesse dei diversi reparti aziendali interessati, da quelli amministrativi e commerciali a quelli dedicati alla logistica.

La digitalizzazione del ciclo dell'ordine

In particolare, se consideriamo le transazioni commerciali nella loro interezza, quale espressione del ciclo attivo e passivo, l'ordine spesso costituisce l'elemento di raccordo tra tutti i documenti connessi alle singole operazioni. Il salto qualitativo nella gestione del ciclo passivo si ottiene soltanto attraverso la capacità di acquisire automaticamente le informazioni digitali contenute nel file XML nei sistemi gestionali e contabili, attraverso delle informazioni chiave da concordare con i propri fornitori e che consentono di legare la fattura con le altre informazioni del ciclo dell'ordine (DDT, contratto, SAL, autorizzazione pagamento), da riportare in determinate sezioni del tracciato informatico SDI, e attraverso le quali si possono automatizzare le fasi di registrazione e contabilizzazione.

La compilazione di tali campi consente di associare le informazioni contenute nella fattura alle informazioni gestionali presenti nei sistemi del ricevente con l'obiettivo di una contabilizzazione automatica, anche ai fini della contabilità industriale e del controllo di gestione delle fatture ricevute.

Oltre a tali dati, le specifiche tecniche dell'Agenzia delle Entrate consentono anche la gestione di informazioni relative alla ricezione dei beni e servizi oggetto della fattura, nonché i dati delle fatture collegate.

In particolare i dati dell'ordine sono indicati nella sezione del tracciato 2.1.2, i dati del contratto nella sezione 2.1.3, i dati che identificano l'avvenuta ricezione della

prestazione/fornitura nella sezione 2.1.5, i dati delle SAL nella sezione 2.1.7, i dati del DDT nella sezione 2.1.8.

Chi intraprende questa strada difficilmente l'abbandona, in quanto acquisisce la consapevolezza che, ogni codifica, scendendo a livello delle informazioni chiave gli porterà benefici enormi in termini di efficienza e di qualità del lavoro, consentendo tempi rapidi di riscontro e di pagamento.

Agli albori della digitalizzazione si è partiti con lo slogan "liberare l'azienda dalla carta" portando a casa i notevoli risparmi in termine di occupazione degli archivi, ricerca dei documenti, disponibilità delle informazioni indipendentemente da chi li aveva prodotte e dal luogo in cui erano precedentemente conservate.

Ora, la mission più elevata da perseguire è di considerare più importante il contenuto che il contenitore, ossia quello di "liberare l'informazione dal veicolo documentale" consentendo di classificarla, trattarla automaticamente e gestirla come elemento di unione fra sistemi gestionali ed amministrativi di partner commerciali creando delle relazioni virtuose digitali rapide ed efficienti.

Tutti elementi che consentono non solo di non subire la fatturazione elettronica, ma di evolvere la professionalità di contabili, amministrativi, controller e commercialisti. Per fare questo non ci si può accontentare di affrontare il tema della fatturazione elettronica in Italia, comprando il primo programma di gestione dell'adempimento, allo scopo di raggiungere l'obiettivo minimo di riuscire a riportare il processo attuale in un XML completo dei campi obbligatori, necessari per i controlli dell'Agenzia delle Entrate. Mentre la competenza normativa si può creare o delegare e la tecnologia o il software si possono comprare, l'innovazione si crea solo con una visione imprenditoriale o consulenziale evoluta e pronta a cogliere le opportunità del cambiamento. Se non cambiamo, non cresciamo. Se non cresciamo, non stiamo davvero facendo impresa.



A.I. e IoT: ESSERE "SMART", MA CON CAUTELA.

La sfida del GDPR nell'utilizzo delle nuove tecnologie



Di **Alessandra Fischetti** e **Paola Gallozzi**
Avvocati
componenti D&L NET

In occasione del DIG.Eat 2019 Alessandra Fischetti e Paola Gallozzi affrontano il lato oscuro delle innovazioni tecnologiche che, prepotentemente, entrano nelle nostre vite, modificando le nostre abitudini. Ecco quali sono le tutele offerte dal GDPR.

A.I. e IoT, un binomio accattivante

L'Intelligenza Artificiale e l'Internet of Things costituiscono un binomio imprescindibile e sempre più accattivante per chiunque. Difficile incontrare qualcuno, soprattutto tra le nuove generazioni, che non utilizzi quotidianamente smartphone, smartwatch o smart speakers. Ma cos'è l'Intelligenza Artificiale? Potremmo definirla come la capacità di un sistema tecnologico di "agire" autonomamente, analizzare e risolvere problemi, compiendo azioni tipiche dell'intelligenza umana. Con l'espressione IoT (*Internet of Things*), cioè *Internet delle cose*, ci si riferisce invece alla possibilità di collegare ad Internet qualunque tipo di oggetto e dispositivo attraverso dei sensori. L'IoT è una sorta di grande network in cui gli oggetti che ci circondano possono essere facilmente connessi alla rete ed interconnessi tra loro. Questi oggetti "intelligenti" (*smart objects*) raccolgono e si scambiano i nostri dati personali in tempo reale, dialogando tra loro e comunicando con il mondo esterno. In altre parole, l'IoT connette i dispositivi che raccolgono i dati che l'A.I. analizza e trasforma in informazioni utili per l'utente che usufruisce degli *smart objects*, ma è anche considerato come il possibile fulcro di decisioni

strategiche per i grandi operatori economici.

I campi di applicazione sono molteplici: si pensi alla smart home (serrature che si aprono e chiudono con lo smartphone, impianti che si possono accendere o spegnere a distanza, frigorifero che segnala scadenze dei cibi), *smart cars*, *smartwatches*, *smart city*, fino agli smart toys per bambini. E poi gli *smart speakers*, con gli assistenti personali intelligenti che imperano nelle nostre case: *“Hey Google, Hey Siri: ditemi chi non conosce la vostra concorrente Alexa!”*

In un mondo sempre più connesso l’IoT, per necessità o anche solo per divertimento, ha consentito e continuerà a consentire la completa digitalizzazione e connessione in rete delle nostre vite, ancora troppo spesso in modo del tutto inconsapevole.

Quanto è diffusa negli utenti la coscienza dei rischi cui di fatto si sottopongono utilizzando smart objects che acquisiscono, registrano ed elaborano dati e abitudini personali? Quanti utenti sono consapevoli del fatto che questi dispositivi consentono di costruire un loro profilo dettagliato, monitorandone i comportamenti al punto di poter giungere a limitare la loro libertà e capacità di autodeterminazione? Probabilmente, in pochi.

Sulla (scarsa) consapevolezza in materia di A.I.:

Convenzione 108 e Linee guida

Non è un caso che, stante la poca cultura diffusa in materia di protezione dei propri dati personali, lo scorso 28 gennaio il Comitato per la protezione dei dati istituito dalla Convenzione n. 108/1981 del Consiglio d’Europa, in occasione della XIII edizione del Data Protection Day, ha pubblicato le “Linee guida sull’intelligenza artificiale e la protezione dei dati”, (<https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>), di fatto, a tutela di tutti quei dati personali inconsapevolmente immessi dai numerosi utilizzatori all’interno di questi sistemi di intelligenza artificiale.

Le linee guida sono, infatti, volte ad assicurare che siano sempre garantiti il rispetto della dignità umana e dei diritti fondamentali dell’individuo, con particolare attenzione al diritto alla protezione dei dati personali. Il testo contiene un espresso invito rivolto ai Legislatori ed ai responsabili politici degli Stati aderenti, affinché gli stessi investano risorse nella formazione e nell’educazione digitale,

al fine evidente di aumentare la generale consapevolezza dei rischi connessi a questi nuovi strumenti (cfr. parte III art. 9). Inoltre, si rivolgono direttamente anche agli operatori del settore affinché, “fin dalla progettazione” e nella successiva fase di diffusione di questi nuovi strumenti, pongano in essere tutte le opportune cautele per garantire il rispetto dei diritti e delle libertà fondamentali dell’individuo, in particolare il diritto alla vita privata, in relazione all’elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati») – cfr. art. 1 Convenzione 108/81 e art. 2 Linee guida 28/01/2019.

La sfida del GDPR nell’uso delle nuove tecnologie

Il recente intervento del Consiglio d’Europa si inserisce nel solco già tracciato dal Legislatore comunitario sfociato nel Regolamento europeo 2016/679 (GDPR). È evidente il richiamo dei principi fondamentali di accountability e “*privacy by design e by default*”, di cui all’art. 25 GDPR, sulla “Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”. Infatti, l’invito agli operatori del settore ad una preventiva analisi dei potenziali rischi per i diritti e le libertà fondamentali degli individui, ai fini di una corretta progettazione degli *smart objects*, richiama una serie di prescrizioni contenute nel GDPR. Prescrizioni che sono certamente applicabili all’IoT e più in generale ai sistemi di A.I., imponendo a tutti i Titolari / Contitolari del Trattamento (ovvero a tutti i soggetti della filiera dei sistemi di A.I. e IoT: sviluppatori, produttori e fornitori di servizi) l’onere di valutare, fin dalla fase di progettazione (*Privacy by design*), i possibili rischi, adottando conseguentemente misure tecniche e organizzative “adeguate”. Il GDPR non impone delle misure minime di sicurezza, ma ne esige un livello costantemente adeguato con il progredire della tecnologia per impostazione predefinita (*Privacy by default*). Il Titolare deve trattare solamente i dati personali nella misura necessaria e sufficiente per il conseguimento delle finalità per le quali sono stati raccolti. Si tratta di un approccio rivoluzionario rispetto al passato, ove il problema “sicurezza dei dati” si valutava solamente a posteriori.

Questo cambio di prospettiva imposto dal GDPR è il suo vero pregio, perché rende la normativa sempre attuale e “al passo coi tempi”, imponendo lo sviluppo contestuale di nuove tecnologie e relative nuove misure di protezione dei dati personali.



HEY YOU HEY YOU



di Massimo Cruciotti

Presidente dell'Associazione
no profit SOS Archivi
[SOS Archivi - www.sosarchivi.it]

10 anni di SOS Archivi:
al DIG.Eat 2019 per tutelare
il nostro patrimonio
culturale

HEY YOU
HEY YOU

In occasione del DIG.Eat 2019 Massimo Cruciotti presenta un contributo sul lato oscuro della tutela del patrimonio archivistico, presentando l'esperienza decennale di SOS Archivi, nata a seguito di un evento catastrofico, che ha permesso di dar vita a un'esperienza costruttiva di collaborazione fra il settore privato e quello pubblico, in un ambito (apparentemente lontano) da quello degli archivi: la gestione dell'emergenza.

Perché SOS Archivi

A seguito del terremoto di L'Aquila, si era venuta a creare la necessità di recuperare gli archivi cartacei rimasti sotto le macerie. Vennero contattate diverse aziende da tutta Italia, che potessero mettere a disposizione il loro know-how e i loro mezzi per questa operazione di salvataggio.

In questo contesto, le aziende che parteciparono agli interventi decisero di unirsi in associazione, dandosi come obiettivo principale quello di riunire professionisti del settore beni culturali per promuovere la prevenzione delle situazioni accidentali che possono danneggiare gli archivi documentali e le biblioteche e per offrire, in caso di necessità, immediato intervento specialistico in situazioni di urgenza. Nacque così SOS Archivi.

Pubblico e privato

Il tema della tutela del patrimonio è molto sentito da coloro che lavorano nell'ambito dei Beni Culturali e non solo, soprattutto dopo le alluvioni e i terremoti

degli ultimi anni. La collaborazione in questo settore è fondamentale, perché diverse figure professionali devono essere coinvolte e lavorare a stretto contatto con archivisti e bibliotecari: restauratori, ingegneri, architetti, risk manager, biologi, geologi, informatici, storici dell'arte. Da qui la nostra volontà di rinnovare, anche per questa edizione, la concessione del nostro patrocinio scientifico al DIG.Eat, l'evento annuale sul digitale, targato ANORC.

L'obiettivo comune è quello di preservare il patrimonio culturale che appartiene a tutti noi, diffondendo una rinnovata cultura archivistica, con una maggiore consapevolezza nei riguardi dei nuovi archivi fatti di bit, di ambito sia pubblico, che privato.

Un territorio a rischio

L'alto rischio idrogeologico a cui è soggetto il nostro Paese, rende particolarmente vulnerabile il nostro patrimonio culturale, specie quello conservato non correttamente in luoghi poco adatti al deposito dei beni. Non parliamo solo di carta: nel corso degli anni sono stati adottati nuovi supporti, nuove forme di conservazione, ma nemmeno la tecnologia è esente dal subire danni imprevisti (basta pensare a cosa può succedere in una server room allagata).

Si è abituati a pensare alla prevenzione come sinonimo di interventi costosi, ma ogni euro speso in prevenzione è speso anche in valorizzazione dei beni e gioca un ruolo fondamentale nella business continuity: formulare ed attuare i piani di sicurezza, mettere in pratica le linee guida fornite dal Ministero dei Beni e delle Attività Culturali (alcune azioni basilari consistono nella creazione di una mappa degli edifici di conservazione e della localizzazione dei beni e dei supporti digitali, nell'organizzare le collezioni in unità conservative idonee, nell'effettuare la manutenzione e la pulizia costante dei locali, etc.), sono atti dovuti se si è custodi di asset da cui dipende una comunità, un'azienda, un ente, o una qualsiasi attività produttiva.

Consapevolezza, collaborazione, comunicazione

In Italia si tende a fare la conta dei danni "in tempo di guerra", piuttosto che la-

vorare sulla messa in sicurezza “in tempo di pace”: una brutta abitudine, che solo negli ultimi anni sta vedendo un cambio di rotta.

Essere consapevoli dei rischi a cui si è esposti, spesso facilmente evitabili, come quelli legati alla disattenzione umana, significa iniziare un percorso virtuoso di prevenzione dei danni e di tutela del patrimonio.

I 10 anni di attività di SOS Archivi posso essere festeggiati grazie all’apporto di conoscenze multidisciplinari che ci ha permesso di promuovere e sviluppare attività informative e comunicative partendo da diversi punti di vista, quello dell’archivista, quello del biologo, quello dell’esperto di cyber security o quello dell’assicuratore: ogni professione svolge il suo ruolo quando si parla di salvaguardia e nessuna è subordinata all’altra.

Un invito a fare rete

Riteniamo che il DIG.Eat sia un evento importante del settore digitale italiano e siamo sempre ben felici di offrire il nostro patrocinio.

Proprio in questa ottica di collaborazione, ci auguriamo che il nostro network di aziende sostenitrici e di professionisti, possa continuare a crescere, per festeggiare di nuovo i prossimi 10 anni e per diffondere la consapevolezza che le catastrofi non si possono prevedere, ma i danni e le perdite che provocano si possono evitare.

Vi invitiamo a visitare il nostro sito, per scoprire come entrare a far parte del nostro network: <https://www.sosarchivi.it>

OUTSIDE THE WALL

OUTSIDE THE WALL



La Geo-ICT italiana al tempo dello Sviluppo Sostenibile

di Sergio Farruggia

Vicepresidente Stati Generali dell'Innovazione
[Stati Generali dell'Innovazione
www.statigeneralinnovazione.it]

In occasione del DIG.Eat 2019 Sergio Farruggia affronta il lato oscuro della cosiddetta Geospatial Revolution, il fenomeno evolutivo della cultura geografica che si fa strada e si accompagna con la trasformazione digitale della società contemporanea.

1. Il mercato geospaziale globale

Le tecnologie geospaziali sono diventate in pochi anni onnipervasive. Tale fenomeno dipende essenzialmente dal continuo e inarrestabile processo di innovazione tecnologica, determinato sia dagli effetti della ricerca nelle Geospatial Sciences, sia dalle "contaminazioni" con un sempre maggior numero di altri settori ICT.

Il settore geospaziale presenta valori economici importanti. Limitandoci alle stime globali, complessivamente è previsto che esso passi dai 292,2 miliardi di dollari del 2017 ai **439,2 miliardi di dollari nel 2020**, con un tasso annuo di crescita nel periodo (*compound annual growth rate, CAGR*) **del 13,6%** -- con una accelerazione di oltre due punti percentuali rispetto al periodo precedente 2013-2017. Ragguardevole risulta l'impatto economico generato dall'utilizzo dei dati e tecnologie geospaziali, esteso oltre i confini dell'industria geospaziale. Viene evidenziato un progresso dai 1.188,7 miliardi di dollari del 2013 ai 2.210,7 miliardi di dollari del 2017, con un CAGR del 20,9%. Ciò dà ragione **del ruolo delle tecnologie geospaziali come elemento trainante nella diffusione dell'innovazione digitale.**

Uno scenario analogo viene illustrato in uno studio sull'impatto economico dei Servizi Geospaziali, commissionato nel 2017 da Google. Questo documento offre un quadro prezioso non solo rispetto al business, ma anche nei riguardi dei benefici per gli utenti e per la società tutta indotti dalla diffusione dei servizi geospaziali. Il report offre in appendice la rappresentazione schematica di tali benefici, valutati a livello globale e per specifiche regioni, tra cui per il nostro Continente: ad esempio, si stima che l'utilizzo delle mappe digitali consenta agli utenti europei benefit complessivi pari a circa 72 miliardi di dollari per anno, riduca i tempi di viaggio mediamente del 10%, traducibile in circa 87 miliardi di dollari risparmiati per anno e permetta un risparmio di circa 3 miliardi di ore per anno, grazie a scelte di acquisto più efficienti, corrispondenti a circa 39 miliardi di dollari risparmiati per anno.

2. Il posizionamento dell'Italia nel mercato del settore geospaziale

Secondo l'analisi comparativa tra 50 nazioni, rispetto al loro grado di maturità e propensione all'utilizzo delle tecnologie geospaziali, espressa in termini di Geospatial Readiness Index (GRI), il nostro Paese presenta una seria impreparazione rispetto al potenziale offerto dal settore geospaziale nei riguardi dell'economia, della salvaguardia dell'ambiente e dello sviluppo sociale.

Questo indicatore è stato concepito per riassumere – attraverso l'assegnazione di un punteggio sintetico - la capacità di sfruttare le opportunità offerte dalle tecnologie geospaziali espressa da una nazione. Per la valutazione del Geospatial Readiness Index (GRI) 2018, ogni nazione è stata esaminata rispetto ai seguenti cinque pillar: (i) Infrastruttura dei dati; (ii) Quadro normativo delle policy; (iii) Capacità istituzionale (Formazione e specializzazioni disponibili); (iv) Livello di adozione della tecnologia da parte degli utenti; (v) Tessuto industriale.

Il punteggio per il GRI 2018 assegnato all'Italia (26,35 punti su cento) ci colloca al diciottesimo posto nelle graduatorie delle 50 nazioni considerate, guadagnando due posizioni rispetto al 2017 -- un segnale positivo. Va inoltre notato come il punteggio ottenuto non si discosti molto da quello di alcuni Paesi che ci pre-

cedono, come Russia (26,96) e Giappone (27,00). Tuttavia, gli Stati del G7 mantengono una posizione migliore del nostro, con USA (67,77) e UK (40,63) leader indiscussi.

Il GRI, disaggregato rispetto ai 5 pilastri considerati, fornisce una fotografia oggettiva dei punti di forza e delle criticità riscontrati per l'Italia: nella seguente tabella sono evidenziati in grassetto gli ambiti che offrono opportunità di miglioramento.

Pillar	Classifica
Infrastruttura dei dati	20a su 50
Quadro normativo delle policy	7a su 50
Capacità istituzionale (Formazione e specializzazioni disponibili)	24a su 50
Livello di adozione della tecnologia da parte degli utenti	20a su 50
Tessuto industriale	11a su 50

Al risultato lusinghiero per le policy adottate e per il livello del "tessuto industriale", che ci posiziona nel gruppo delle nazioni leader per questi aspetti, si contrappongono gli esiti insoddisfacenti relativamente agli altri tre pilastri. Assai penalizzante –anche perché ostacola la penetrazione delle soluzioni abbinate alle "non Geo" ICT e la diffusione di Spatial Data Infrastructure appropriate- risulta la readiness in tema di "Formazione": l'Italia è citata tra le nazioni che hanno "strong science and research, and academia courses" ma risente, secondo questa indagine, di un'offerta insufficiente di percorsi formativi più prossimi alle esigenze delle imprese e dei settori applicativi, criticità che posiziona il nostro Paese al 24° posto. Sia di esempio l'India che, in 26a posizione in termini di GRI complessivo, ha ottenuto per lo stes-

so pillar il 17° posto: ciò denota attenzione al tema e investimenti adeguati, con l'obiettivo di migliorare quanto prima la readiness della nazione.

3. Colmare il gap e ricoprire una posizione consona a un membro del G7

Dal quadro tratteggiato nei punti precedenti, **risulta fondamentale lo sviluppo di condizioni che stimolino l'utilizzo delle tecnologie geospaziali oltre i contesti "tradizionali"**, in combinazione con le sempre più numerose altre componenti e processi ICT (quarto pillar). A questo riguardo, si può ricorrere agli strumenti per le policy riguardanti l'Earth Observation e l'Innovazione, di cui l'Italia si è dotata, specificatamente: il Piano nazionale di supporto al Programma europeo Copernicus all'interno del Piano Space Economy e il Piano nazionale Impresa 4.0. L'industria geospaziale nazionale è all'altezza della sfida: essa detiene ruoli di prestigio a livello internazionale, come quello delle imprese della Earth Observation Technology, supportate anche da risultati di eccellenza della ricerca del settore.

Allo stesso tempo, è urgente attuare campagne di sensibilizzazione e azioni di supporto volte a **incrementare la quantità e soprattutto la qualità –ad iniziare dalla appropriata assegnazione delle licenze d'uso- dei dataset e dei servizi geospaziali**, iniziando a monitorare la disponibilità dei dati territoriali a livello urbano, quello di maggior dettaglio e quindi di maggior pregio in termini di riuso. Controllo sistematico che deve includere l'osservazione dell'attuazione della "Direttiva del parlamento europeo e del consiglio relativa al riutilizzo dell'informazione del settore pubblico", per le categorie di dati geospaziali di elevato valore, elencati nel Progetto di Risoluzione Legislativa del Parlamento Europeo (Relazione sulla proposta 7.12.2018). Per il buon esito delle precedenti azioni risulta indispensabile **introdurre nei processi smart city/community le figure professionali relative alla Geographic Information normate dal 2018 (Norma UNI 11621-5)**, quindi atte a procedura di certificazione. In particolare, coinvolgere il Geographic Information Manager, figura professionale inserita negli organismi di governance di un'organizzazione per sostenere e governare l'uso consapevole dei dati geografici e delle tecnologie disponibili per la loro raccolta, gestione e condivisione, con particolare attenzione anche allo sviluppo delle Spatial Data Infrastructure.



MONEY

di Andrea Broglio - Avvocato, esperto Privacy

In occasione del DIG.Eat 2019, Andrea Broglio affronta il lato oscuro della protezione dei dati. Il “professionista della privacy” non deve esclusivamente adempiere alle varie attività previste dal GDPR, ma deve considerare il mondo esterno come una realtà che cambia freneticamente, comprendendo le varie dinamiche che stanno modificando le nostre abitudini e stili di vita.

*“Have your baggage and passport ready and then follow the green line to customs and immigration. BA flight 215 to Rome, ...”
... “Live for today, gone tomorrow, that’s me.”*

Lo dico subito: sono un novizio.

Non ho mai partecipato al DIG.Eat e mi preparo così alla mia prima volta, a scoprire il lato oscuro del digitale.

Il sottofondo musicale è in ogni caso eccellente.

Sono un novizio anche di digitale.

Diventato giovanotto nel secolo scorso, ero restio ad abbandonare la penna per digitare, ecco, appunto, su una tastiera, i miei testi. Ora, passati molti anni, fatico, se non uso la penna per qualche giorno, a riprenderla con scioltezza; le mie giornate trascorrono, per lavoro, davanti a uno schermo e a una tastiera.

L’elettronica ha preso il sopravvento, in un continuo, incessante progredire, quasi il ritmo fosse stato, davvero, previsto magicamente dai suoni metallici delle monete che ascoltiamo in Money.

Sono un novizio anche in *data protection*.

Se non fosse stato, un paio di anni fa, per un amico e cliente che mi chiedeva lumi sull'approssimarsi del GDPR, oggi, forse, non sarei un "professionista della privacy".

Devo quindi dire grazie a questo amico, in realtà per tante, tantissime cose ma anche per il fatto che, dovendo adeguare la sua società alle nuove disposizioni, mi ha aperto, letteralmente, un mondo.

Un mondo che oggi esploro avido di conoscenza.

Un mondo, anche, che in realtà, avevo davanti e tutto intorno da tempo e nel quale ero immerso ma che non guardavo, non capivo.

Oggi direi: *Data (Money), it's a gas!*

Oggi, in realtà guardo, cerco di comprendere, di capire, da un altro punto di vista. Oggi mi rendo conto, o almeno penso, che la strada per comprendere, per analizzare, per gestire tutto questo sia ancora molto lunga. Ma affascinante, estremamente affascinante.

Non si tratta solo di verificare, capire le lacune delle organizzazioni che i clienti mi sottopongono e, in un'ottica debitamente responsabilizzata e trasparente, di aiutarli ad adempiere alle diverse prescrizioni, a redigere e tenere le documentazioni, i registri e quant'altro.

Oggi, penso, si tratta di capire, al di là degli adempimenti di legge o di Regolamento, anche di quelli che verranno, come una realtà e un mondo che cambiano freneticamente potranno diventare.

Si tratta di capire come e quanto ci cambieranno queste nuove realtà, anche se lo hanno già fatto in modo penetrante, modificando via via abitudini e stili di vita.

I cambiamenti sono stati notevoli; le opportunità e le nuove possibilità altrettanto. Fino a qualche tempo fa era difficile poter pensare di gestire un viaggio, per esempio, senza andare fisicamente in un'agenzia.

Accadeva, siamo sinceri, fino a qualche tempo fa.

Oggi viaggiamo con i biglietti del treno e le prenotazioni dell'albergo in tasca, elettroniche.

Oggi la penna per firmare un foglio di carta la utilizziamo sempre meno. Sono esempi banali. O forse non tanto se pensiamo alla velocità con la quale sono diventati realtà "comune" e quante cose che oggi non lo sono, diventeranno, in ancora più breve tempo, altrettanto "comuni".

Come gestiremo il futuro, questo futuro e quello che ancora non sappiamo cosa ci porterà, anche se un po' ce lo immaginiamo, dipenderà da noi, da ciascuno e da tutti.

Nella tumultuosa, velocissima società che stiamo vivendo, sempre più governata da algoritmi e bit che sono sempre più parte di noi e delle cose che utilizzeremo, toccheremo, guarderemo, avremo addosso e intorno, credo che capire, comprendere e analizzare come l'uomo dovrà gestire il progresso sarà fondamentale.

Penso che, in fondo, la cosa più importante sarà saper distinguere, pensare e capire. Sentire, in senso "sentimentale", quello che un'operazione matematica, pur estremamente complessa, non potrà mai sentire.

È ormai certo, tanto per accennare un aspetto, che l'automazione sostituirà molti lavori e che ciò avverrà piuttosto in fretta.

È ancora da capire quale sarà il modo per far sì che il fattore umano continui ad avere un ruolo significativo, determinante.

Per non essere travolti, ma, soprattutto, per continuare a esercitare il nostro diritto di scegliere.

Us and Them

"It can't be helped but there's a lot of it about

With, without

And who'll deny it's what the fighting's all about

Out of the way, it's a busy day

I've got things on my mind".

Comprendere, analizzare e studiare, senza mai dimenticare la nostra natura e le nostre prerogative, che sono fatte e costituite anche di sentimenti ed emozioni, sarà ciò che ci consentirà di essere, e fare, la differenza.

Mi viene in mente HAL 9000 e la filastrocca che i suoi creatori gli insegnarono. Mi viene in mente, subito dopo (e così ora ascolto, con un veloce click sul p.c.), la voce potente, lirica, sublime e irripetibile di *Clare Torry in The Great Gig in the Sky*. Tanto "umana", tanto meravigliosa, tanto sentimentale. Voglio credere, voglio continuare a credere che una macchina possa suggerirmela, in base a calcoli e valutazioni, perché forse sono o sarò in un determinato mood sentimentale.

Voglio (pretendo) di poter continuare a scegliere se e quando ascoltarla.

MONEYMONEYMONEYMONEY
MONEYMONEYMONEY
MONEYMONEYMONEYMONEY

WHEN YOU'RE IN

Potenzialità e criticità connesse
al trattamento elettronico
delle Informazioni in ambito sanitario



di Maurizio Lombardi

Vicepresidente e Responsabile Formazione
e Comunicazione A.IT.A.S.I.T.

(Associazione Italiana Amministratori
di Sistemi Informativi e Telemedicina

www.aitasit.org



In occasione del DIG.Eat 2019 Maurizio Lombardi affronta il lato oscuro della rivoluzione innescata dalla dematerializzazione, invitando a riflettere sui rischi e sulle implicazioni che un tale sistema di gestione delle informazioni inevitabilmente comporta, con particolare riguardo alla protezione dei dati.

Anche in ambito sanitario si sente sempre più spesso parlare di informatizzazione e digitalizzazione, ma contrariamente a quello che si potrebbe superficialmente pensare, questi concetti non fanno riferimento ad una moda momentanea. Al contrario rispondono al preciso dovere di tutte le Pubbliche Amministrazioni di dematerializzare i processi attraverso i quali erogano i propri servizi ai cittadini.

Quando si parla di “dematerializzazione”, si fa riferimento a un fenomeno che ha fatto la sua prima comparsa negli anni Ottanta del secolo scorso, irrompendo anzitutto nel mondo economico-finanziario, per indicare la progressiva perdita di consistenza fisica dei titoli di credito al fine di superarne la fisicità consentendone così forme di circolazione virtuali.

Gli obiettivi che oggi si pone “il fenomeno” dell’innovazione sono sostanzialmente i seguenti:

- miglioramento dell’efficienza dei processi attraverso il perseguimento di un cambiamento organizzativo basato sulle potenzialità offerte dall’innovazione tecnologica;

- miglioramento della cooperazione fra Pubbliche Amministrazioni attraverso la condivisione delle informazioni contenute negli archivi con lo scopo di ridurre i tempi delle procedure e semplificare la fruibilità delle stesse da parte dei cittadini;
- miglioramento dell'efficienza e della trasparenza della spesa pubblica;
- sviluppo di servizi on line che consentano un più veloce e facile accesso alle prestazioni anche da parte dei cittadini maggiormente svantaggiati a causa di condizioni sociali sfavorevoli;
- aumento della possibilità di misurare la qualità dei servizi offerti attraverso l'accesso a dati che ne consentano la valutazione dell'impatto sia da un punto di vista quantitativo che qualitativo oltre che del grado di soddisfazione relativa ai servizi stessi da parte dei cittadini.

A fronte di tali (e ben noti) benefici non ci si interroga mai abbastanza sui rischi e sulle implicazioni che un tale sistema di gestione delle informazioni inevitabilmente comporta. La tanto invocata Privacy, vale la pena di ricordarlo, è solo uno degli aspetti relativi alle modalità e alla sicurezza con cui ci si deve necessariamente confrontare.

Altro equivoco di cui, troppo spesso e con superficialità, si minimizzano le implicazioni è quello generato dalla *paternità* del dato. Anche se in formato digitale, le informazioni che quotidianamente gestiamo, con ruoli diversi, continuano ad appartenere solo ed unicamente al soggetto di riferimento e perciò l'incarico al trattamento, implica diversi obblighi relativi a trasparenza e sicurezza, con l'attuazione di tutta una serie di misure, nel rispetto delle finalità e degli obiettivi già concordati con l'utente al momento della sottoscrizione dell'apposito consenso.

Un altro aspetto estremamente significativo è quello relativo alle policy di accesso al sistema informativo. Oltre alle già note disposizioni in materia di sicurezza relative alle caratteristiche imprescindibili con cui ogni password dovrebbe esse-

re scelta, è di fondamentale diversificare, sulla base delle competenze di ciascun utente, i profili di accesso. È necessario differenziare le azioni che un determinato operatore può o non può fare, nei riguardi del patrimonio informativo che il sistema gestisce. L'attribuzione di una policy di accesso inoltre dovrebbe essere solo lo step iniziale del percorso di abilitazione di un operatore alla gestione del patrimonio informativo.

Da queste considerazioni emerge come diretta conseguenza l'importanza della tracciabilità di tutte le operazioni che il sistema deve prevedere e garantire (siano esse una semplice consultazione o una modifica di una o più informazioni). In qualunque momento dovrà essere quindi possibile risalire a "chi ha fatto cosa" e quando.

In virtù di quanto sopra esposto in Aitasit riteniamo che la formazione sia lo strumento più efficace per preparare e aggiornare adeguatamente chi ha accesso ad un patrimonio così prezioso com'è quello rappresentato dall'insieme delle informazioni sanitarie dei cittadini. Formazione che deve prevedere interventi differenziati a seconda delle peculiarità dei ruoli che ogni operatore ricopre all'interno del network sanitario.



SPEAK TO ME SPEAK TO ME

La consulenza della firma olografa e grafometrica



di Antonella Foi, grafologa
Referente formazione
Dipartimento peritale
AGI [Associazione Grafologica Italiana
www.a-g-i.it]

In occasione del DIG.Eat 2019 Antonella Foi affronta il lato oscuro del valore legale della firma all'indomani della rivoluzione digitale, riflettendo sul ruolo del grafologo, chiamato ad intervenire per verificare l'autografia o la falsità di una sottoscrizione (sia olografa che grafometrica).

La firma è unica per ognuno di noi

La scrittura può essere definita come un atto motorio prodotto dall'interazione di fenomeni nervosi, centrali e periferici che si esprimono ad opera di effettori. Tra questi, la mano rappresenta quello più comunemente usato.

L'atto dello scrivere, al pari di qualsiasi espressione della motricità, necessita di meccanismi di controllo tra loro interconnessi e portano gli impulsi propriocettivi dagli effettori periferici alla corteccia cerebrale sensoriale.

Esistono due tipi di circuiti di controllo motorio: circuito chiuso (closed loop) e circuito aperto (open loop).

Il primo agisce nella fase di apprendimento, quando il bambino traccia le prime lettere e le migliora correggendo via via gli errori segnalati da un feedback propriocettivo e/o estero-cettivo, oppure quando un falsario riproduce una firma non sua e modifica il movimento mentre è in atto, comparandolo al modello da riprodurre.

Il circuito aperto, invece, entra in gioco quando il movimento appreso viene memorizzato in una traccia mnemonica che può essere utilizzata in situazioni analoghe, senza più bisogno di feedback.

Esso consente azioni motorie anche molto veloci ma, non disponendo di un feedback correttivo, esclude la possibilità di correzione.

L'esempio tipico di un gesto sottoposto a controllo motorio a circuito aperto è la firma vergata di getto.

La modalità di esecuzione viene memorizzata sotto forma di un programma archiviato nella memoria a lungo termine e potrà essere richiamata ogni qualvolta si renda necessario.

Sono questi i presupposti neurofisiologici che consentono di attribuire alla firma il valore legale attribuitole dall'art. 2702 C.C.

L'esame ed il confronto

La firma rivela in modo accentuato l'individualità dello scrivente; la sua esecuzione è riconducibile al circuito di controllo aperto pertanto risulta massimamente automatizzata.

Tuttavia, come l'organismo, la firma cambia fisiologicamente nel tempo e per eventuali effetti di patologie intercorrenti. Pertanto, il grafologo deve tenere conto dell'età e dello stato clinico dello scrivente.

In ogni caso, una volta stabilizzata, la firma conserva la sua dinamica esecutiva, pur con alcune diversità formali.

Come prescrive il protocollo, l'esame di una firma olografa parte dall'ispezione del supporto e dello strumento scrittorio, prosegue con l'esame del gesto grafico per verificarne naturalezza e spontaneità (cioè credibilità), osservando la complessità del tracciato e utilizzando i segni di velocità come indicati da vari autori.

Stabilita la natura della sottoscrizione, il perito indirizzerà l'attenzione alla dinamica esecutiva attraverso le caratteristiche che la descrivono.

Molta attenzione rivolgerà a quei gesti, talora poco appariscenti, che connotano in modo peculiare la firma.

Dopo aver esaminate le comparative nel medesimo modo, il consulente dovrà occuparsi del confronto evidenziando le concordanze sostanziali che, anche in presenza di qualche differenza spiegabile oggettivamente, consentiranno di orientare il giudizio all'autografia; se, al contrario, prevarranno le differenze, la firma sarà apocrifia anche se formalmente simile.

Scopo del falsario, infatti, è di riprodurre il più fedelmente una firma altrui e per far ciò può scegliere tra l'imitazione pedissequa o la riproduzione libera.

Nel primo caso, utilizzerà il circuito chiuso di controllo motorio che gli consente di correggere via via eventuali errori e quindi procederà lentamente, lasciando nel tratto i segni del rallentamento e delle eventuali soste.

Nella riproduzione libera, a circuito aperto di controllo motorio, eseguirà velocemente e di getto un tracciato che non è il suo, ma inevitabilmente si lascerà sfuggire qualche caratteristica che non appartiene alle autografe da riprodurre, ma al suo specifico automatismo.

Un caso particolare è la dissimulazione della propria firma; in questo caso l'autore cercherà di produrre un esemplare che, pur differenziandosi da quelli consueti, possa comunque conservare un aspetto credibile, in modo da indurre chi lo osserva a ritenerlo autografo.

L'esperto osserverà le caratteristiche minute, poiché il firmatario difficilmente riuscirà a svincolarsi completamente dai propri automatismi.

La firma immateriale

La grande diffusione della firma grafometrica rende concreto il rischio che si debba stabilire l'autografia di un esemplare sconosciuto.

Il protocollo da seguire non si discosterà da quello utilizzato nel caso di firma cartacea, ma utilizzerà tutte le risorse offerte dal software per analizzare le movenze del tracciato al fine di stabilirne la naturalezza e coglierne le caratteristiche salienti.

Il compito del perito sarà enormemente facilitato, potendo attingere ai dati numerici che descrivono in ogni punto pressione, velocità, accelerazione/decelerazione e posizione nel campo grafico del tratto rispetto agli assi di riferimento, puntando l'attenzione sulle parti ritenute più significative.

Il percorso potrà essere animato e consentirà di seguirne il divenire, così come è stato eseguito. Particolarmente interessanti si riveleranno i percorsi della penna - entro qualche millimetro di distanza dal piano - quando interrompe il contatto con la tavoletta.

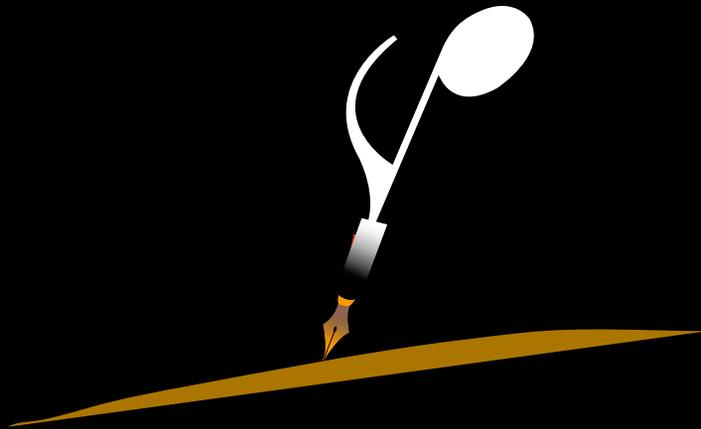
Nell'esame e nel confronto con esemplari autografi, raccolti con strumen-

tazione analoga ma, se necessario, anche olografi, ogni grafologo forense saprà puntare l'attenzione su quei parametri che meglio evidenzieranno la vera natura della mano scrivente.

Conclusioni

La Consulenza Tecnica e la Perizia su firme richiedono indubbiamente un approccio specialistico da parte di Grafologi forensi (disciplinati dalla legge n. 4 del 14.01.2013), con una preparazione approfondita e soggetti a continuo aggiornamento.

Attualmente essi possono certificare le proprie competenze professionali - anche riguardo l'esame delle firme grafometriche - con AICQ-SICEV, Organismo di terza parte accreditato da ACCREDIA, cui l'Associazione Grafologica Italiana si è rivolta in favore di tutti i grafologi forensi.



BRING THE BOYS BACK HOME



di Armando Zambrano

Ingegnere – Presidente del CNI
Consiglio Nazionale degli Ingegneri
www.tuttoingegnere.it

In occasione del DIG.Eat 2019 Armando Zambrano affronta il lato meno conosciuto della professione digitale, presentando una riflessione sull'evoluzione dell'Ordine in chiave 4.0. La digitalizzazione e le nuove tecnologie impattano in maniera considerevole su diversi settori dell'Ingegneria, andando ad influenzare, non ultimo, le scelte professionali dei neo-laureati.

Da tempo il Consiglio Nazionale Ingegneri dedica un'attenzione crescente al fenomeno della digitalizzazione e delle nuove tecnologie, ciò anche in considerazione del forte impatto che questi fenomeni stanno avendo per il nostro stesso Ordine.

Nel 2017 su 25.731 laureati in Ingegneria di primo livello, ben 7.210 hanno seguito un corso di laurea in Ingegneria dell'informazione (28%); ciò ha comportato un mutamento significativo anche nella platea dei nostri iscritti. Basti pensare che, sulla base degli ultimi dati disponibili, su 241.791 iscritti all'Albo, ben 146.344 lo sono anche per il settore dell'Ingegneria dell'informazione, oltre il 60%.

Il tema della digitalizzazione è però trasversale, ed interessa tutti i settori dell'ingegneria.

Nel settore civile ed ambientale, tutti i processi di progettazione e di costruzione sono investiti ormai dall'impatto della modellazione informativa. Il Piano Industria 4.0 ha favorito la diffusione nel nostro sistema produttivo delle nuove tecnologie dell'informazione e della digitalizzazione, riconoscendo

negli Ingegneri una figura centrale per l'implementazione di tali processi. Su entrambi i fronti (modellazione e Industria 4.0) il CNI, in collaborazione con la sua Fondazione, ha realizzato diverse iniziative di formazione e aggiornamento professionale a favore degli Iscritti all'Albo.

Le nuove tecnologie dell'informazione favoriscono, peraltro, il formarsi di nuovi profili professionali altamente specialistici che necessitano di certificazione, a tutela principalmente dei committenti. Anche per questo il CNI ha promosso la nascita dell'Agenzia CertING, per la certificazione delle competenze degli ingegneri.

Senza contare che il digitale costituisce l'ambiente naturale per la nascita e lo sviluppo di nuove forme di servizio agli iscritti, come ad esempio WorkING, la piattaforma del CNI dedicata all'incontro tra offerta e domanda di posizioni professionali riservate agli ingegneri.

È anche per questo che abbiamo accolto con favore la richiesta di patrocinio dell'evento DIG.Eat 2019.



ONE OF MY TURNS

Club TI Milano e l'avanzamento Digitale in Italia

ONE OF MY TURNS



di Ornella Fouillouze

Vicepresidente e Coordinatore
Gruppo Sanità di ClubTI Milano
[ClubTI Milano - www.clubtimilano.net]



In occasione del DIG.Eat 2019 la dott.ssa Fouillouze affronta il lato oscuro dell'attivismo a livello associazionistico, presentando una riflessione sulle attività svolte in prima linea da ClubTI, anche sulla scorta della collaborazione pluriennale con ANORC, che ha motivato la partecipazione alla XII edizione del DIG.Eat.

Il **ClubTI** di Milano, Club per le Tecnologie dell'Informazione, è stato fondato nel 1987 ed è una libera e spontanea **associazione di professionisti di ICT** che esercitano competenze manageriali, tecnologiche, organizzative e di consulenza. Fa parte, con altre iniziative territoriali simili, della rete FIDA Inform, di cui ClubTI Milano è tra i fondatori.

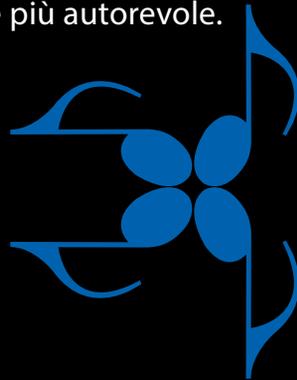
I soci (CIO, manager dell'offerta, uomini del marketing), sono portatori delle più diverse esperienze sulla trasformazione digitale e sulle strategie d'impresa, rappresentando un valore d'opinione in grado di incidere anche sul contesto ICT del Paese. Il Club TI rappresenta una **voce professionale ed autorevole** nei confronti delle istituzioni sui temi riguardanti la tecnologia dell'informazione.

Club TI segue gli aspetti innovativi di interesse per la comunità ICT e organizza eventi specifici; negli ultimi 5 anni il tema chiave è la **trasformazione digitale**, che viene declinata sia per ambiti tecnologici che per mercati. Ad esempio, nel

mercato della **Sanità Digitale** viene organizzato il premio biennale eHealth4all (www.ehealth4all.it). Si tratta di un riconoscimento alla **migliore applicazione digitale per la prevenzione**, nato nel 2015 in Expo ed ora alla sua terza edizione. Un altro esempio sul piano tecnologico, invece, è il tema **blockchain**, in cui Club TI ha accumulato una forte expertise sul tema e organizza eventi e seminari.

Sui temi più affini alle iniziative ANORC, Club TI Milano ha seguito, negli anni, la problematica dell'archiviazione sostitutiva e della completa **dematerializzazione**. A partire dal 2017 ha iniziato a seguire con continuità il tema **dell'Identità Digitale**, organizzando eventi e workshop sul tema dell'uso e della crescita di SPID. A fine marzo 2019 Club TI ha dato vita a un gruppo di lavoro dal titolo **#ClubTI4SPID**, che segue il tema dell'Identità digitale, anche nell'ottica dell'avanzamento digitale del Paese (vedi indice DESI e posizionamento europeo).

La richiesta e l'auspicio è quindi di collaborare sempre più strettamente con ANORC per avere, insieme, una voce più autorevole.



THE THIN ICE

Il lato oscuro del pensiero umano: l'illusione della conoscenza



THE THIN ICE



di Edoardo Guastamacchia

Presidente Associazione Medici Endocrinologi

e Daniela Agrimi

Responsabile Telemedicina e Sanità
Digitale AME

[Associazione Medici Endocrinologi

www.associazionemediciendocrinologi.it]

In occasione del DIG.Eat 2019, Daniela Agrimi e Edoardo Guastamacchia affrontano il lato oscuro del pensiero umano, in una riflessione incentrata sul progredire dell'innovazione e sui rischi derivati dal prevaricare di una super intelligenza imminente. La rete riuscirà a prevaricare la nostra capacità di pensare e agire?

Internet è diventato un compagno di vita, ci fornisce una fonte, apparentemente inesauribile, di informazioni, è una colonna portante nella comunità della conoscenza. La tecnologia dell'informazione, a fronte di molte semplificazioni, ha aumentato però paure e indotto preoccupanti conseguenze, come **l'autostima cognitiva**.

L'innovazione sta progredendo così velocemente da rendere l'ipotesi di una superintelligenza imminente, un pericolo che si autoalimenta e prevaricherà la nostra capacità di pensare e agire. **Una super intelligenza è più temibile e nociva di una conoscenza sommaria?**

La possibilità di fare ricerche in rete ha aumentato la nostra autostima cognitiva, cioè l'impressione di essere in grado di ricordare e di elaborare informazioni. Studi condotti nell'ambito delle scienze cognitive indicano come persone invitate a svolgere ricerche su internet, circa un determinato quesito, stimavano la propria capacità di rispondere a domande non collegate in misura più alta rispetto a coloro che non dispongono di internet per la ricerca. L'accessibilità immediata alle

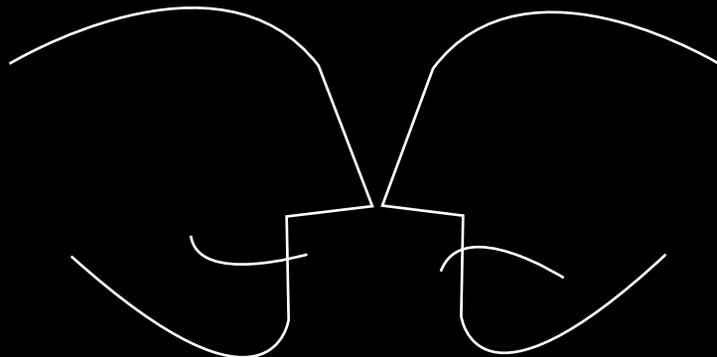
informazioni attraverso la navigazione Wi-Fi, ci restituisce la sensazione di avere tutto il sapere sulla punta delle dita e, quindi, nel nostro cervello.

Siamo tutti esperti?

Un esempio viene offerto da WebMD, una applicazione medica, in lingua inglese, disponibile su AppStore. Con la funzione Symptom Checker è possibile selezionare la parte del corpo da indagare, scegliere i sintomi e conoscere le malattie potenziali. Ad oggi conta 62.312 recensioni tra cui questa "Fantastico ci ha azzeccato subito con più di una diagnosi (che nemmeno il mio medico di base...!) È richiesta una avanzata conoscenza della lingua inglese. Inutile dare una stella solo perché non si capisce!!!".

In letteratura sono riportati studi sull'esperienza di medici, infermieri e pazienti che hanno sviluppato autodiagnosi con WebMD o siti simili. Le conclusioni restituiscono un margine di errore alto, i pazienti con autodiagnosi web-mediata non ne sanno molto di più dei pazienti che non hanno interpellato internet, ma si pregiano di una alta conoscenza medica, spesso non accettano la diagnosi o inseguono terapie alternative. Ciò è stato evidenziato anche per i temi della finanza, con rilevanti perdite economiche nella simulazione degli investimenti del gruppo web-mediato.

La nostra intelligenza non alberga nei singoli cervelli, bensì in una mente collettiva e connettiva, il lato in chiaro del pensiero umano.



ROUND AND AROUND

Il ruolo attivo di AssoSoftware al fianco delle imprese:
il caso della fatturazione elettronica



di Roberto Bellini

Direttore generale di AssoSoftware
(www.assosoftware.it)

In occasione del DIG.Eat 2019 Roberto Bellini affronta il lato oscuro dell'innovazione d'impresa, esprimendo la vision di AssoSoftware rispetto all'attuale evoluzione dello scenario nazionale, con particolare riguardo all'introduzione della Fatturazione Elettronica.

AssoSoftware è da sempre molto attenta ai processi di innovazione del Paese e anche nel caso della Fattura Elettronica ha svolto e continua a svolgere, grazie al know-how delle software house associate, un ruolo attivo e propositivo su tutti i tavoli tecnici e normativi, collaborando con il MEF, l'Agenzia delle Entrate e tutti gli stakeholder, per agevolare l'avvio e la messa a regime del nuovo obbligo. Alla luce di queste premesse, AssoSoftware non poteva che concedere, anche per questa edizione, il proprio patrocinio morale all'evento DIG.Eat di ANORC, garantendo la propria partecipazione a presidio del settore.

Sulla strada della digitalizzazione, la Fatturazione elettronica rappresenta un passo fondamentale non solo per recuperare gettito dalla lotta all'evasione (2 mld di euro all'anno di maggiori entrate), ma soprattutto per far compiere uno scatto in avanti all'efficienza delle imprese nella gestione dei loro processi interni grazie all'elaborazione dei dati presenti nelle fatture e alla riconciliazione dei medesimi con le altre informazioni aziendali. **Con la Fatturazione elettronica in**

primis, e poi con la dematerializzazione dell'intero ciclo dell'ordine, si può puntare alla massima integrazione dei processi e degli strumenti aziendali, riducendo le fasi manuali ed eliminando qualsiasi ostacolo che impedisca gli automatismi e rallenti le attività. **L'integrazione è dunque il fattore chiave della digitalizzazione che porterà alle imprese e al sistema Italia i benefici evidenziati da tutti gli osservatori, non ultimo una maggiore competitività.**

Un primo bilancio dell'avvio dell'e-Fattura, che, come ogni disruptive innovation, comporta il cambiamento di abitudini consolidate e l'emergere di alcune criticità, è sostanzialmente positivo. In questa fase AssoSoftware è stata in prima linea per mettere a disposizione gratuita delle aziende associate, e di tutti gli attori coinvolti, strumenti, soluzioni e buone pratiche per consentire loro di trarre il massimo vantaggio da questa importante innovazione.

**R
O
U
N
D

A
N
D

A
R
O
U
N
D**



CREDEMTEL 30 ANNI

DA 30 ANNI AFFIDABILITÀ ED INNOVAZIONE A SUPPORTO DEL TUO LAVORO



A NEW MACHINE

FATTURA ELETTRONICA: UNA RIVOLUZIONE A META'



di Marco Cuchel

Presidente ANC

[Associazione Nazionale Commercialisti

www.ancnazionale.it]

In occasione del DIG.Eat 2019 Marco Cuchel affronta il lato oscuro della fatturazione elettronica, analizzando i risvolti del cambiamento apportato dalla sua introduzione, con particolare riferimento agli aspetti legati alla tutela e alla riservatezza delle informazioni sensibili di imprese e contribuenti. L'Associazione Nazionale Commercialisti ha da subito rappresentato un punto di riferimento per i professionisti del settore.

Il 2019, con l'introduzione della fattura elettronica, segna un cambiamento significativo del nostro sistema fiscale e del suo funzionamento. La fatturazione elettronica costituisce una innovazione con la quale sono chiamati a confrontarsi i professionisti economici e milioni di contribuenti tra cittadini e imprese, che pone numerosi e importanti aspetti, alcuni dei quali ancora oggi devono essere affrontati e risolti dall'Amministrazione Finanziaria. L'Associazione Nazionale Commercialisti ha rappresentato da subito alle istituzioni e al legislatore italiani le gravi criticità delle nuove procedure, in particolare i rischi rispetto alla tutela e alla riservatezza delle informazioni sensibili di imprese e contribuenti. Rischi che hanno trovato conferma nell'intervento da parte dell'Autorità Garante per la privacy nei confronti dell'Agenzia delle Entrate la quale è stata quindi chiamata ad apportare dei correttivi per evitare il verificarsi di comportamenti impropri a danno dei soggetti coinvolti.

L'ANC non ha mancato di esprimere preoccupazione rispetto al fatto che grandi soggetti economici privati si trovino a custodire, trattare e profilare informazioni che possono essere oggetto di operazioni commerciali, con il

rischio di compromettere il sistema economico nazionale nel suo complesso.

La vulnerabilità delle nuove procedure sul piano della riservatezza delle informazioni costituisce, a nostro avviso, insieme alle altre criticità del sistema, un'emergenza da risolvere nell'interesse della collettività.

I commercialisti non sono contrari alla modernizzazione e al cambiamento, anzi per il ruolo che rivestono da sempre accompagnano cittadini e imprese nei processi di digitalizzazione e informatizzazione del Paese, riteniamo però che i cambiamenti vadano governati con accortezza e che sulle misure fiscali la categoria sia in grado di apportare un contributo utile.

INTERSTELLAR OVERDRIVE

Chi governa il digitale?



di Francesco Antoniol

Vice Presidente di Arch.I.M.

[Associazione Archivisti in Movimento]

In occasione del DIG.Eat 2019 Francesco Antoniol affronta il lato oscuro della libera professione al tempo della transizione digitale, in particolare di quella che si ritiene essere la figura centrale rispetto all'intero processo: l'archivista, ossia colui che progetta l'organizzazione della memoria. Che significato assume questa professione oggi?

Riflettere sul processo della transizione digitale, sui principi, sulle regole e sui procedimenti che la dovrebbero condurre in porto equivale necessariamente al ripensamento del ruolo e della figura che vi dovrebbe sovrintendere, **l'archivista**.

Anche se la norma ha disegnato la via alla digitalizzazione italiana ormai da qualche tempo, è la definizione della figura centrale in questo processo che, tutt'oggi, è incerta, in divenire, preda della mediazione tra le fughe delle richieste del mercato, in cui domina una disincantata libera professione, e le pause dettate da una più lenta e riflessiva visione istituzionale animata, anche in senso positivo, da un sentimento dai toni, molto spesso, marcatamente beniculturalisti.

Siamo però, probabilmente, al momento della resa dei conti. In questi giorni è stato reso pubblico lo schema di decreto ministeriale relativo alla procedura per la formazione dell'elenco nazionale che vedrà iscritta, tra le altre

figure, anche quella dell'archivista.

Non è questo il momento per dibattere sulle numerose perplessità sollevate dalla innovativa proposta ma piuttosto è auspicio che il DIG.Eat si configuri come la sede di un costruttivo confronto che veda il delinarsi della figura **dell'archivista come quella di colui che progetta l'organizzazione della memoria a partire da una solida percezione del presente corroborata da una visione aperta agli stimoli di ciò che sarà e non, troppo, limitata da ciò che è stato.**

Il modo complesso di fare l'archivista oggi, di essere archivista, è conoscenza di mondi laterali e convergenti (dalla sicurezza informatica all'universo privacy, dagli utilizzi del linguaggio XML alla metadattazione, dai metodi di trasmissione del documento al confronto con la norma europea, solo per citarne alcuni) che non sono la sola tassonomia archivistica con cui, peraltro, è necessario il confronto per una feconda sintesi che deve rappresentare, definitivamente, il ruolo e la coscienza dell'archivista di oggi e di domani.



G. Moscara